第35号

交通运输部关于发布《电子收费 单片式车载单元(OBU)技术要求》的公告

为加快推动高速公路电子不停车快捷收费应用，交通运输部组织制定了《电子收费 单片式车载单元(OBU)技术要求》，现予以公布，自公布之日起施行。

该技术要求的管理权和解释权归交通运输部，日常解释和管理工作由主编单位交通运输部公路科学研究院负责。请各有关单位在实践中注意总结经验，及时将发现的问题和修改意见函告交通运输部公路科学研究院(地址：北京市海淀区西土城路8号，邮

政编码100088)，以便修订时参考。

交通运输部

2019年5月21日

电子收费 单片式车载单元（OBU）
技术要求

2019 年 5 月

目　录

1 范围

本技术要求规定了电子不停车收费（ETC）系统中单片式车载单元（OBU）设备要求、OBE-SAM、典型交易流程、测试方法等方面的内容。

本技术要求适用于公路和城市道路电子收费系统，自动车辆识别、车辆出入管理等领域可参照使用。

2 规范性引用文件

下列文件中的条款通过本技术要求的引用而成为本技术要求的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本技术要求。凡是不注日期的引用文件，其最新版本适用于本技术要求。

GB/T 2423.5—1995 电工电子产品环境试验 第二部分：试验方法 试验 Ea 和导则：冲击

GB/T 2423.10—2008 电工电子产品环境试验 第 2 部分：试验方法 试验 Fc：振动（正弦）

GB 8897.4—2008 原电池 第 4 部分：锂原电池的安全要求

GB/T 16649 识别卡带触点的集成电路卡

GB/T 17618 信息技术设备 抗扰度限值和测量方法

GB/T 17626.2 电磁兼容 试验和测量技术 静电放电抗扰度试验

GB/T 18655 车辆、船和内燃机无线电骚扰特性用于保护车载接收机的限值和测量方法

GB/T 20135—2006 智能运输系统 电子收费 系统框架模型

GB/T 20839—2007 智能运输系统 通用术语

GB/T 20851.1 电子收费 专用短程通信 第 1 部分：物理层

GB/T 20851.2 电子收费 专用短程通信 第 2 部分：数据链路层

GB/T 20851.3 电子收费 专用短程通信 第 3 部分：应用层

GB/T 20851.4 电子收费 专用短程通信 第 4 部分：设备应用

GB/T 20851.5 电子收费 专用短程通信 第 5 部分：物理层主要参数测试方

法

GM/T 0008　安全芯片密码检测准则

《收费公路联网收费技术要求》（交通部 2007 年第 35 号公告）

《收费公路联网电子不停车收费技术要求》（交通运输部 2011 年第 13 号公告）

UL1642　美国锂电池安全标准

UN38.3（Rev.5） 联合国危险物品运输试验和标准手册 38.3 款

ISO/IEC 7816　识别卡——带触电的集成电路卡

3　术语、定义和缩略语

3.1 术语和定义

GB/T 20135—2006 和 GB/T 20839—2007 界定的术语和定义适用于本技术要求。

3.1.1 ETC 门架系统

在高速公路沿线断面建设的，具备通行费分段计费、车牌图像识别等功能的专用设施。

3.1.2 开放式收费制式

将高速公路全线划分为若干路段，各路段内分别计算费额的收费制式。

3.1.3 自由流收费

应用电子收费技术自动完成对多条车道上自由行驶车辆收费的方式，又称多车道自由流收费方式。

3.1.4 开放式自由流收费

采取开放式收费制式的自由流收费方式。

3.1.5 通行凭证

路侧单元（RSU）与单片式 OBU 交易后所产生的具有不可抵赖性的用于后台记账形式扣费和结算等应用的凭证。

3.2 缩略语

下列缩略语适用于本技术要求。

CPU——中央处理器（Central Processing Unit）

DSRC——专用短程通信（Dedicated Short Range Communication）

ETC——电子收费（Electronic Toll Collection）

FID ——文件标识（File Identifier）

MAC——信息鉴别码（Message Authentication Code）

OBE——车载设备（On Board Equipment）

OBE-SAM ——车载设备安全控制模块（On Board Equipment-Security Access Module）

OBU——车载单元（On Board Unit）

RSU——路侧单元（Roadside Unit）

RS232——串行通信接口（Serial Communication Interface）

SM4——国产密码算法 SM4

SPI——串行外设接口（Serial Peripheral Interface）

UI——无编号信息（Unnumbered Information）

3DES——三重数据加密标准（Triple Data Encryption Standard）

4 设备要求

4.1 产品形态

单片式 OBU 可有多种产品形态，如一体化产品、分体式产品、嵌入式模块等。

4.2 关键技术指标

4.2.1 无线通信链路

单片式 OBU 和 RSU 之间的 DSRC 通信协议应符合 GB/T 20851.1～GB/T

20851.3 的规定。

4.2.2 休眠机制

在 ETC 应用下单片式 OBU 响应 VST 后或建立专用链路后对本 OBU 的专用链路地址的下行链路数据帧的超时等待时间应不小于 300ms，超时后可进入休眠状态。

4.2.3 其他

单片式 OBU 的唤醒灵敏度、等效全向辐射功率在符合 GB/T 20851.1 规定的前提下可具备调节功能。

4.3 功能

4.3.1 应用接口

4.3.1.1 基本要求

单片式 OBU 与 RSU 之间的 ETC 应用接口应符合 GB/T 20851.4 的规定。

为支持单片式 OBU 应用，对应用层服务原语 ACTION 扩展接口，新增 GetTollData 原语和 SetTollData 原语，其中 ActionType 扩展定义：

——ActionType = 5：GetTollData；

——ActionType = 6：SetTollData。

4.3.1.2 GetTollData 原语

4.3.1.2.1 功能

本原语用于完成 OBU 和 RSU 之间的双向认证，并可对返回的信息进行完整性保护。GetTollData 默认获取 OBU 中“ETC 应用车辆信息文件”，“入 / 出口信息文件”根据实际应用场景可选。

4.3.1.2.2 接口

4.3.1.2.2.1 请求（GetTollData.request）

GetTollData.request 参数要求见表 4-1。

表4-1 GetTollData.request参数要求

参数	取值	参数说明
mode	TRUE	确认模式，需应答
did	Dsrc-DID	ETC应用等于1
actionType	5	等于5
accessCredentials	OCTET STRING (SIZE(0..127,...))	可选

actionParameter	GetTollDataRq::=SEQUENCE{
	fillBIT BIT STRING (SIZE(4)),
	transType OCTET STRING (SIZE(1)),
	vehicleInfo RangeOfFile,
	tollInfo RangeOfFile OPTIONAL,
	rndRSE Rand OPTIONAL,
	keyIdForAC INTEGER(0..255) OPTIONAL,
	keyIdForAuthen INTEGER(0..255)OPTIONAL
	}
		填充位
		交易类型
		待读取的车辆信息范围
		待读取的过站信息范围
		随机数，若存在，OBU响应authenticator
		访问许可认证密钥标识
		信息鉴别密钥版本

iid	—	不存在

其中 accessCredentials 由 RSU 对 8 字节 rndOBE 加密计算得到，计算方法参见 GB/T 20851.4 中“8.2 访问许可”。

其中 RangeOfFile 的 ASN.1 定义如下：

```
RangeOfFile::=SEQUENCE{
    offset   INTEGER(0.. 32767,...),--读取偏移量
    length   INTEGER(0..127,...)   --读取长度
    }
```

4.3.1.2.2.2 应答（GetTollData.response）

GetTollData.response 参数要求见表 4-2。

表4-2 GetTollData.response参数要求

参数	取值	参数说明
did	Dsrc-DID	ETC应用对应1

responseParameter	GetTollDataRs::=SEQUENCE {
	fillBIT BIT STRING (SIZE(6)),
	vehicleInfo File,
	tollInfoFile OPTIONAL,
	authenticator OCTET STRING(SIZE(8)) OPTIONAL
	}
		填充位
		车辆信息
		过站信息
		鉴别码

iid	—	不存在
ret	ReturnStatus	必备

其中 authenticator 可用于 RSU 对 OBU 的身份认证，同时对车辆信息和过站信息（可选）进行完整性保护。authenticator 的计算域为车辆信息（vehicleInfo）和待读取的本次过站信息（tollInfo，如果存在）。计算方法参见 GB/T 20851.4 中“8.3 信息鉴别”。

4.3.1.3 SetTollData 原语

4.3.1.3.1 功能

该原语实现获取 OBU 计算的 TAC 及写入过站信息，其中过站信息写入可根据实际应用场景可选。

4.3.1.3.2 接口

4.3.1.3.2.1 请求（SetTollData.request）

SetTollData.request 参数要求见表 4-3。

表4-3 SetTollData.request参数要求

参数	取值	参数说明
mode	TRUE	确认模式，需应答
did	Dsrc-DID	ETC应用等于1
actionType	6	等于6
accessCredentials	OCTET STRING (SIZE(0..127,...))	可选

actionParameter	SetTollDataRq::=SEQUENCE{
	fillBIT BIT STRING (SIZE(6)),
	rndRSE Rand,
	tacPara TacPara,
	tollInfo PartOfFIle OPTIONAL
	keyIdForAC INTEGER(0..255) OPTIONAL，
	keyIdForAuthen INTEGER(0..255)
	}
		填充位
		用于计算authenticator的随机数
		TAC计算参数
		待写入的本次过站信息
		访问许可认证密钥标识
		信息鉴别密钥版本

iid	—	不存在

其中 accessCredentials 由 RSU 对 8 字节 rndOBE 加密计算得到，计算方法参见 GB/T 20851.4 中“8.2 访问许可”。

TAC 码计算参数的 ASN.1 类型定义为：

```
TacPara::=SEQUENCE{
        transAmount     OCTET STRING (SIZE(4)),
        transType       OCTET STRING (SIZE(1)),
        terminalID      OCTET STRING (SIZE(6)),
        transSN         OCTET STRING (SIZE(4)),
        transTime       OCTET STRING (SIZE(7)),
        transStationID  OCTET STRING (SIZE(3))
}
```

PartOfFile 的 ASN.1 类型定义为：

```
PartOfFile::=SEQUENCE{
```

```
offset          INTEGER(0..32767,...),
length          INTEGER(0..127,...),
fileContent     File
}
```

4.3.1.3.2.2 应答（SetTollData.response）

SetTollData.response 参数要求见表 4-4。

表4-4 SetTollData.response参数要求

参数	取值	参数说明
did	Dsrc-DID	ETC应用对应1

responseParameter	SetTollDataRs::=SEQUENCE{
	tacInfo OCTET STRING (SIZE(4)),
	authenticator OCTET STRING (SIZE(8))
	}
		TAC码
		鉴别码

iid	—	不存在
ret	ReturnStatus	必备

其中 authenticator 的计算域为 TAC 计算参数（tacPara）、车型（vehicleClass）及写入的本次过站信息（tollInfo，如果存在）。计算方法参见 GB/T 20851.4 中“8.3 信息鉴别”。

注：SetTollData 原语亦可通过 accessCredentials 和 authenticator 完成 RSU 和 OBU 的双向认证，可用于其他交易流程。

4.3.2 部件

单片式 OBU 可选的部件：扬声器、蜂鸣器、字符显示器、红绿指示灯、RS232 串口、蓝牙通讯模块、ISO/IEC 14443 接口模块等。

4.3.3 信息存储

单片式 OBU 内的用户信息存储宜采用数据块的方式，寻址应采用目录和文件的方式。

4.3.4 应用的更新

单片式 OBU 应支持应用更新。

4.3.5 防拆卸与恢复

单片式 OBU 应具备防拆卸功能，一旦被拆卸，应当立即将单片式 OBU 内

的相应信息存储区设置标志字节 / 标志位。

因拆卸而引起的 ETC 应用失效应能通过软件设置的方式得到恢复。

4.3.6 自检功能

单片式 OBU 应具备故障报警功能。电池供电的单片式 OBU 还应具备低电报警功能。

4.3.7 安装位置

对于一体化单片式 OBU，小型客、货车宜安装在车辆的前挡风玻璃上方居中（后视镜位置附近）位置，预先在前挡风玻璃留有微波窗口的车辆，宜安装在微波窗口位置，大型客、货车宜安装在前风挡玻璃下方居中位置。对于分体式、嵌入式等单片式 OBU，安装位置应不影响其正常通信。

4.4 人机交互

单片式 OBU 应具备状态提示功能，应包括“交易正常”、“交易异常”、“设备低电”等情况。

当采用蜂鸣器实现声音提示功能时，响音模式应为：

——收到 SetMMIRq 指示内容为“正常”时，一声短促“嘀”；

——收到 SetMMIRq 指示内容为“异常”时，三声短促“嘀”；

——OBU 自检到低电或故障时，一声长“嘀”；

——其他情况，不响。

4.5 性能

4.5.1 电磁兼容

对于连接在车辆线束上或车载电源上的单片式 OBU，其无线电骚扰特性应符合 GB/T 18655 的规定，限值符合等级 3 要求或符合整车生产商要求。

单片式 OBU 静电放电抗扰度应符合 GB/T 17618 性能判据 B 的规定。

4.5.2 可靠性

单片式 OBU 可靠运行时间不小于 5 年。

4.6 外部接口

单片式 OBU 可根据需要设置外部接口。

具备外部接口的单片式 OBU 应具备保护电路，以避免外部连接对设备内置电池造成损坏。

4.7 安全要求

单片式 OBU 应符合以下安全要求：

1　应提供安全访问模块（OBE-SAM），以存放访问控制密钥和 ETC 应用信息等，具体要求见第 5 章；

2　应用安全应符合 GB/T 20851.4 中第 8 章相关规定。单片式 OBU 的访问权限应满足以下要求：

a) RSU 第一次发送带有专用链路地址的下行链路数据帧的服务原语时应携带访问许可；

b) 单片式 OBU 在通过访问许可认证后，RSU 具备对 OBU 的访问权限。

4.8 供电

单片式 OBU 可采取电池、车载电源、电池加车载电源等供电方式。单片式 OBU 电池应具备相应的安全性，并符合 GB 8897.4-2008（锂原电池）、UL 1642 和 UN 38.3 的规定。电池应标识制造商名称，商标名或商标，生产日期，型号，正 / 负极，电压等。

采用电池供电的一体化单片式 OBU 应提供太阳能或其他的补电方式。

4.9 环境条件

环境条件应符合以下要求：

1　工作温度：-25℃～+85℃，寒区-40℃～+85℃。

2　存储温度：-20℃～+55℃。

3　相对工作湿度：5%～100%。

4　振动：应符合 GB/T 2423.10—2008 附录 C 中表 C.1 第三行给出的设备应用严酷等级要求，频率范围 10Hz～150Hz，加速度 10m/s²，在每一轴线方向上的扫频循环次数为 20。

冲击：应符合 GB/T 2423.5—1995 第 5 章中表 1 第三行给出的严酷等级要求，峰值加速度 300m/s²，相应的标称脉冲持续时间 18ms，相应的速度变化量半正弦为 3.4m/s。

5　OBE-SAM

5.1 一般规定

OBE-SAM 的基本功能应符合下列规定：

1　支持多应用，各应用之间相互独立。

2　支持多种文件类型，包括二进制文件、定长记录文件、变长记录文件、循环文件。

3　在通信过程中支持多种安全保护机制（信息的机密性和完整性保护）。

4　支持多种安全访问方式和权限。

5　支持 SM4 算法。

6　支持拆卸状态设定功能。

7　应用安全机制应符合本技术要求附录 A 的有关规定。

8　采用 SOP8 封装形式，具体尺寸和引脚定义应符合本技术要求附录 B 的有关规定。

5.2 基本参数要求

OBE-SAM 的基本参数符合下列规定：

1　用户数据区非易失性存储器容量应不低于 32kbytes。

2　应支持 ISO/IEC 7816 T=0 通信协议。

3　ISO/IEC 7816 接口在不高于 7.5MHz 外部工作时钟频率下应能正常工作。当外部时钟频率为 3.57MHz 时，通信速率应不低于 115200bit/s。

4　可支持 SPI 通信方式，通信速率应不低于 3Mbit/s。

5　电源电压应支持 1.8V～3.6V 工作电压。

6　其他物理特性、电气特性应符合 GB/T 16649《识别卡带触点的集成电路卡》的规定。

7　安全等级应达到 GM/T 0008《安全芯片密码检测准则》规定的 2 级及以上级别。

8　应通过具备相关资质的第三方安全评估测试。

5.3 文件结构

5.3.1 文件结构图

OBE-SAM 文件结构见图 5-1。

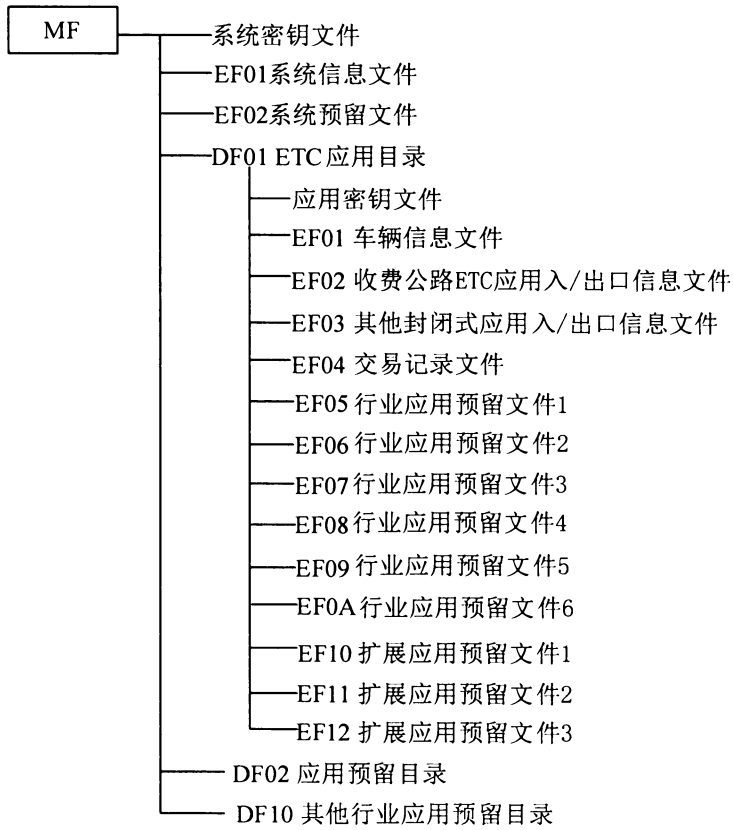


图 5-1 OBE-SAM文件结构

OBE-SAM 详细文件结构应符合表 5-1 的规定：

表 5-1 OBE-SAM 详细文件结构

文件名称	文件类型	文件标识符	读权	写权	备注
MF	主文件	3F00	建立权：MK_{MF}		厂商交货时已经建立
系统密钥文件	密钥文件	—	禁止	增加密钥权：MK_{MF}	禁止读，通过系统主控密钥 MK_{MF} 采用密文+MAC 方式写入密钥
系统信息文件	二进制文件	EF01	自由	$DAMK_{MF}$	自由读，写时使用系统维护密钥 $DAMK_{MF}$ 进行线路保护（明文+ MAC）
系统预留文件	二进制文件	EF02	自由	$DAMK_{MF}$	自由读，写时使用系统维护密钥 $DAMK_{MF}$ 进行线路保护（明文+ MAC）
DF01 ETC 应用目录	目录文件	DF01	建立权 MK_{MF}	擦除权 MK_{MF}	卡主控密钥 MK_{MF} 认证通过后可以建立和擦除文件
应用密钥文件	密钥文件	—	禁止	增加密钥权 MK_{DF01}	禁止读，通过应用主控密钥 MK_{DF01} 采用密文+MAC 方式写入密钥
ETC 应用车辆信息文件	二进制文件	EF01	认证读	$DAMK_{DF01}$	使用 $OPNK11_{DF01}$、$OPNK12_{DF01}$、$OPNK21_{DF01}$ 或 $OPNK22_{DF01}$ 外部认证后读，写时使用应用维护密钥 $DAMK_{DF01}$ 进行线路保护（明文+ MAC）
收费公路 ETC 应用入 / 出口信息文件	二进制文件	EF02	自由	$OPNK11_{DF01}$ 或 $OPNK12_{DF01}$	自由读，使用 $OPNK11_{DF01}$ 或 $OPNK12_{DF01}$ 外部认证后写
其他封闭式应用入 / 出口信息文件	二进制文件	EF03	自由	$OPNK21_{DF01}$ 或 $OPNK22_{DF01}$	自由读，使用 $OPNK21_{DF01}$ 或 $OPNK22_{DF01}$ 外部认证后写
交易记录文件	循环定长记录文件	EF04	自由	任一条 OPNK	自由读，使用 $OPNK11_{DF01}$、$OPNK12_{DF01}$、$OPNK21_{DF01}$ 或 $OPNK22_{DF01}$ 外部认证后写。每条记录 30 字节，200 条记录
行业应用预留文件 1	二进制文件	EF05	自由	$DAMK_{DF01}$	自由读，写时使用应用维护密钥 $DAMK_{DF01}$ 进行线路保护（明文+ MAC）

行业应用预留文件 2	二进制文件	EF06	自由	自由	自由读，自由写
行业应用预留文件 3	二进制文件	EF07	自由	认证写	自由读，外部认证 $UK1_{DF01}$ 通过后可以写，无线路保护
行业应用预留文件 4	二进制文件	EF08	自由	$DAMK_{DF01}$	自由读，写时使用应用维护密钥 $DAMK_{DF01}$ 进行线路保护（明文+ MAC）
行业应用预留文件 5	二进制文件	EF09	自由	自由	自由读，自由写
行业应用预留文件 6	二进制文件	EF0A	自由	认证写	自由读，外部认证 $UK2_{DF01}$ 通过后可以写，无线路保护
扩展应用预留文件 1	二进制文件	EF10	自由	$DAMK_{DF01}$	自由读，写时使用应用维护密钥 $DAMK_{DF01}$ 进行线路保护（明文+ MAC）
扩展应用预留文件 2	二进制文件	EF11	自由	自由	自由读，自由写
扩展应用预留文件 3	二进制文件	EF12	自由	认证写	自由读，外部认证 $UK3_{DF01}$ 通过后可以写，无线路保护

注：1. 所有预留文件分为行业应用预留文件和扩展应用预留文件，行业应用预留文件作为将来行业统一定义使用；扩展应用预留文件为其他应用统一使用。

2. 各省（区、市）不得自行更改统一定义的文件类型、空间长度和操作权限等，同时不得自行定义和使用文件中的行业预留字节，所有预留字节初始化时应写为 0xFF。

3. MF 文件下的应用目录文件标识符，DF02 作为省级应用预留，初始应用主控密钥为 16 字节 0x22；DF10 作为其他行业应用预留使用，初始应用主控密钥为 16 字节 0x10；其他应用目录文件标识符作为交通运输行业应用预留，各省（区、市）不得自行使用。

5.3.2 文件结构详细说明

5.3.2.1 系统信息文件

系统信息文件详细说明见表 5-2。

表5-2 系统信息文件说明

文件标识（FID）			‘EF01’
文件类型			二进制文件
文件长度			99 字节
读取：自由			写入：$DAMK_{MF}$ 线路保护（明文+MAC）
字节	类型	长度（字节）	内容
1～8	cn	8	发行方标识，见《收费公路联网电子不停车收费技术要求》 第二部分 1 关键信息编码
9	cn	1	协约类型
10	cn	1	合同版本

11～18	cn	8	合同序列号
19～22	cn	4	合同签署日期 格式：CCYYMMDD
23～26	cn	4	合同过期日期 格式：CCYYMMDD
27	B	1	拆卸状态，应符合表 5-3 的规定。
28～99	an	72	预留
注：（1）省内不得自行扩展该文件长度。			

拆卸状态说明见表 5-3。

表5-3 拆卸状态说明

字节	值	状态	描述
高 4 位	0000	RS	由路侧根据防拆信息控制 OBU 的通行
	0001	OB	由 OBU 根据防拆信息设置自身工作状态
	1111	NU	防拆信息未启用
	其他		保留
低 4 位	0000	PF	标签已被非法拆卸
	0001	OK	正常工作状态
	其他		保留

5.3.2.2 MF 下系统预留文件

MF 下系统预留文件详细说明见表 5-4。

表5-4 MF下系统预留文件说明

文件标识（FID）			‘EF02’
文件类型			二进制文件
文件长度			512 字节
读取：自由			写入：DAMK$_{MF}$线路保护（明文+MAC）
字节	类型	长度（字节）	内容
1～512	字母数字	512	预留

5.3.2.3 ETC 应用车辆信息文件

ETC 应用车辆信息文件详细说明见表 5-5。

表5-5 ETC应用车辆信息文件说明

文件标识（FID）		‘EF01’
文件类型		二进制文件
文件长度		79 字节
读取：任一条 OPNK		写入：DAMK $_{DF01}$线路保护（明文 + MAC）
字节	长度（字节）	内容
1～12	12	车牌号，全牌照信息，采用字符型存储，汉字采用 GB2312 码，如：“京”编码为“BEA9”；牌照信息不足 12 字节，后补 0x00

13～14	2	车牌颜色 高字节：0x00 低字节：0x00 –蓝色；0x01–黄色；0x02 –黑色；0x03 –白色；0x04-渐变绿色；0x05-黄绿双拼色； 0x06-蓝白渐变；0x07～0xFF 保留
15	1	车型，在《收费公路联网收费技术要求》表 4.3 基础上，参照 JT/T489《收费公路车辆通行费车型分类》，新增定义如下： ①客车车型： 0x33–一类客车；0x34–二类客车；0x35–三类客车；0x36–四类客车；0x37～0x3C–保留。 ②货车车型： 0x3D–一类货车；0x3E–二类货车；0x3F–三类货车；0x40–四类货车；0x41–五类货车；0x42–六类货车；0x43～0x46–保留。 ③专项作业车车型： 0x47–一类专项作业车；0x48–二类专项作业车；0x49–三类专项作业车；0x4A–四类专项作业车；0x4B–五类专项作业车；0x4C–六类专项作业车；0x4D～0x50–保留。
16	1	车辆用户类型，编码方式应符合 GB/T 20851.4《电子收费 专用短程通信 设备应用》的有关规定，应急救援车辆定义为：0x1A；货车列车或半挂汽车列车定义为：0x1B
17～20	4	车辆尺寸（长[2 字节]×宽[1 字节]×高[1 字节]），单位：dm
21	1	车轴数
22	1	车轮数
23～24	2	轴距，单位：dm
25～27	3	车辆核定载重/座位数，其中，载重的单位为：kg
28～43	16	车辆特征描述
44～60	17	车辆识别代码
61～79	19	保留字段

5.3.2.4 收费公路 ETC 应用入 / 出口信息文件说明

收费公路 ETC 应用入 / 出口信息文件详细说明见表 5-6。

表5-6 收费公路ETC应用入 / 出口信息文件说明

文件标识（FID）		‘EF02’
文件类型		二进制文件
文件长度		64 字节
读取：自由		写入：使用 $OPNK11_{DF01}$ 或 $OPNK12_{DF01}$ 外部认证后写
字节	长度（字节）	内容
1～2	2	入/出口收费路网号，见《收费公路联网收费技术要求》表 4.3
3～4	2	入/出口收费站号，见《收费公路联网收费技术要求》表 4.3
5	1	入/出口收费车道号，见《收费公路联网收费技术要求》表 4.3
6～9	4	入 / 出口时间，UNIX 时间，从格林威治标准时间 1970 年 1 月 1 日 0 时 0 分 0 秒起至现在的总秒数，不包括闰秒。

10	1	车型，见表 5-5
11	1	入出口状态，见《收费公路联网收费技术要求》表 4.3
12～23	12	车牌号，全牌照信息，采用字符型存储，汉字采用 GB2312 码，如：“京”编码为“BEA9”；牌照信息不足 12 字节，后补 0x00
24	1	车牌颜色，0x00 –蓝色；0x01–黄色；0x02 –黑色；0x03 –白色；0x04-渐变绿色；0x05-黄绿双拼色； 0x06-蓝白渐变；0x07～0xFF 保留
25	1	货车列车和半挂汽车列车轴数
26～29	4	车辆尺寸（长[2 字节]×宽[1 字节]×高[1 字节]），单位：dm
30～33	4	总重，单位：kg
34～64	31	预留

5.3.2.5 其他封闭式应用入 / 出口信息文件

其他封闭式应用入 / 出口信息文件详细说明见表 5-7。

表5-7 其他封闭式应用入 / 出口信息文件说明

文件标识（FID）		‘EF03’
文件类型		二进制文件
文件长度		64 字节
读取：自由		写入：使用 $OPNK21_{DF01}$ 或 $OPNK22_{DF01}$ 外部认证后写
字节	长度（字节）	内容
1～64	64	预留

5.3.2.6 交易记录文件

交易记录文件详细说明见表 5-8。

表5-8 交易记录文件说明

文件标识（FID）		‘EF04’
文件类型		循环定长记录文件
文件长度		30 字节×200 条记录
读取：自由		写入：任一条 OPNK
字节	长度（字节）	内容
1～4	4	交易金额
5	1	交易类型
6～11	6	终端机编号
12～15	4	终端交易序号
16～22	7	交易时间
23～25	3	ETC 门架编号/收费站编号
26～30	5	预留

5.3.2.7 行业应用预留文件 1

行业应用预留文件 1 详细说明见表 5-9。

表5-9 行业应用预留文件1说明

文件标识（FID）			‘EF05’
文件类型			二进制文件
文件长度			512 字节
读取：自由			写入：DAMK $_{DF01}$ 线路保护（明文 + MAC）
字节	类型	长度（字节）	内容
1～512	字母数字	512	预留

5.3.2.8 行业应用预留文件 2

行业应用预留文件 2 详细说明见表 5-10。

表5-10 行业应用预留文件2说明

文件标识（FID）			‘EF06’
文件类型			二进制文件
文件长度			512 字节
读取：自由			写入：自由
字节	类型	长度（字节）	内容
1～512	字母数字	512	预留

5.3.2.9 行业应用预留文件 3

行业应用预留文件 3 详细说明见表 5-11。

表5-11 行业应用预留文件3说明

文件标识（FID）			‘EF07’
文件类型			二进制文件
文件长度			512 字节
读取：自由			写入：外部认证 UK $_{DF01}$ 通过后可以写，无线路保护
字节	数据元	长度（字节）	内容
1～512	字母数字	512	预留

5.3.2.10 行业应用预留文件 4

行业应用预留文件 4 详细说明见表 5-12。

表5-12 行业应用预留文件4说明

文件标识（FID）			‘EF08’
文件类型			二进制文件
文件长度			512 字节
读取：自由读			写入：DAMK $_{DF01}$ 线路保护（明文 + MAC）
字节	数据元	长度（字节）	内容
1～512	预留	512	预留

5.3.2.11 行业应用预留文件 5

行业应用预留文件 5 详细说明见表 5-13。

表5-13 行业应用预留文件5说明

文件标识（FID）			‘EF09’
文件类型			二进制文件
文件长度			128 字节
读取：自由			写入：自由
字节	数据元	长度（字节）	内容
1～128	预留	128	预留

5.3.2.12 行业应用预留文件 6

行业应用预留文件 6 详细说明见表 5-14。

表5-14 行业应用预留文件6说明

文件标识（FID）			‘EF0A’
文件类型			二进制文件
文件长度			128 字节
读取：自由			写入：外部认证 UK_{DF01} 通过后可以写，无线路保护
字节	数据元	长度（字节）	内容
1～128	预留	128	预留

5.3.2.13 扩展应用预留文件 1

扩展应用预留文件 1 详细说明见表 5-15。

表5-15 扩展应用预留文件1说明

文件标识（FID）			‘EF10’
文件类型			二进制文件
文件长度			512 字节
读取：自由			写入：$DAMK_{DF01}$ 线路保护（明文 + MAC）
字节	数据元	长度（字节）	内容
1～512	预留	512	预留

5.3.2.14 扩展应用预留文件 2

扩展应用预留文件 2 详细说明见表 5-16。

表5-16 扩展应用预留文件2说明

文件标识（FID）			‘EF11’
文件类型			二进制文件
文件长度			512 字节
读取：自由			写入：自由
字节	数据元	长度（字节）	内容

1～512	预留	512	预留

5.3.2.15 扩展应用预留文件 3

扩展应用预留文件 3 详细说明见表 5-17。

表5-17 扩展应用预留文件3说明

文件标识（FID）			‘EF12’
文件类型			二进制文件
文件长度			512 字节
读取：自由			写入：外部认证 UK_{DF01} 通过后可以写，无线路保护
字节	数据元	长度（字节）	内容
1～512	预留	512	预留

5.4 OBE-SAM 密钥规定

OBE-SAM 内密钥结构应符合表 5-18 的规定。

表5-18 OBE-SAM内密钥结构

密钥	说明	密钥用途	密钥标识	错误计数器	密钥长度
MF 下安全文件					
MK_{MF}	MF 系统主控密钥	00H	40H	0FH	10H
$DAMK_{MF}$	MF 系统维护密钥	01H	41H	0FH	10H
DF01 下安全文件					
MK_{DF01}	DF01 应用主控密钥	00H	40H	0FH	10H
$DAMK_{DF01}$	DF01 应用维护密钥	01H	41H	0FH	10H
$UK1_{DF01}$	DF01 外部认证密钥 1	00H	41H	0FH	10H
$UK2_{DF01}$	DF01 外部认证密钥 2	00H	42H	0FH	10H
$UK3_{DF01}$	DF01 外部认证密钥 3	00H	43H	0FH	10H
$OPNK11_{DF01}$	收费公路 ETC 访问许可密钥 1	00H	44H	-	10H
$OPNK21_{DF01}$	其他封闭式应用访问许可密钥 1	00H	45H	-	10H
$OPNK12_{DF01}$	收费公路 ETC 访问许可密钥 2	00H	46H	-	10H
$OPNK22_{DF01}$	其他封闭式应用访问许可密钥 2	00H	47H	-	10H
LTK_{DF01}	鉴别码计算密钥	02H	41H	-	10H
$TACK_{DF01}$	DF01 TAC 计算密钥	03H	40H	-	10H

注：1. 密钥标识的高四位为算法标识：‘4’ - SM4。

2. 系统主控密钥在自身的控制下更新（密文+MAC）。

3. 系统主控密钥外部认证通过后，可在 MF 下进行文件创建。

4. 系统维护密钥在系统主控密钥线路保护控制下装载、更新。

5. 系统维护密钥用于 MF 区域的应用数据维护。

6. 应用主控密钥在系统主控密钥的线路保护控制下装载（密文+MAC）。

7. 应用主控密钥在自身的控制下更新（密文+MAC）。

8. 应用下其它密钥在应用主控密钥的线路保护控制下装载、更新（密文+MAC）。

9. 应用主控密钥外部认证通过后，可以在 DF01 目录下进行文件创建。

10. 应用维护子密钥用于 DF01 应用下的应用数据维护。

11. 所有密钥的装载和修改应使用密文+MAC 的方式。

OBE-SAM 的密钥用途应符合表 5-19 的规定。

表5-19 OBE-SAM密钥管理

分类	密钥	用途
主控密钥	$MK_{\_MF}$	控制 MF 下文件的建立和密钥的写入
	$MK_{\_DF01}$	控制 DF01 下文件的建立和密钥的写入
维护密钥	$DAMK_{\_MF}$	发卡方或应用提供方用于产生更新二进制文件或记录命令的 MAC
	$DAMK_{\_DF01}$	
外部认证密钥	$UK_{\_DF01}$	用于获得相应文件的更新权限
OBU 访问认证密钥	OPNK	用于 RSU 获得对 OBU 的访问权限，不设错误次数限制
鉴别码计算密钥	LTK	用于计算鉴别码
TAC 计算密钥	$TACK_{\_DF01}$	用于产生车道交易 TAC

5.5 OBE-SAM 复位信息的约定

OBE-SAM 复位信息中历史字节的约定（共 15 字节）应符合表 5-20 的规定。

表5-20 OBE-SAM复位信息的约定

名称	类型	长度（字节）	说明
交通运输部标识	an	1	固定为’4A’
芯片商注册标识号	an	2	芯片厂商注册标识
OBU 厂商标识	an	2	由收费公路电子收费密钥管理单位分配
COS 版本号	an	1	主版本号+次版本号，范围 1.0～9.9（双片式） 主版本号+次版本号，范围 A.0～A.F（单片式） B.0～F.F 预留
COS 修订版本号	cn	1	范围 0～99
YEAR	cn	1	生产年份
MON	cn	1	生产月份
DAY	cn	1	生产日
OBE-SAM 结构版本	cn	1	OBE-SAM 结构版本号
流水号	an	4	惟一性（在卡商内部）

6 典型交易流程

6.1 基本要求

RSU 与 OBU 的交易流程依据收费场景分为开放式自由流收费交易流程、封闭式交易流程。

6.2 开放式自由流收费交易流程

6.2.1 交易流程框架

开放式自由流收费交易流程划分为通信链路建立、收费数据（车辆信息）获取、通行凭证获取、用户提示和链路释放五个主要阶段，其交易流程如图 6-1 所示。

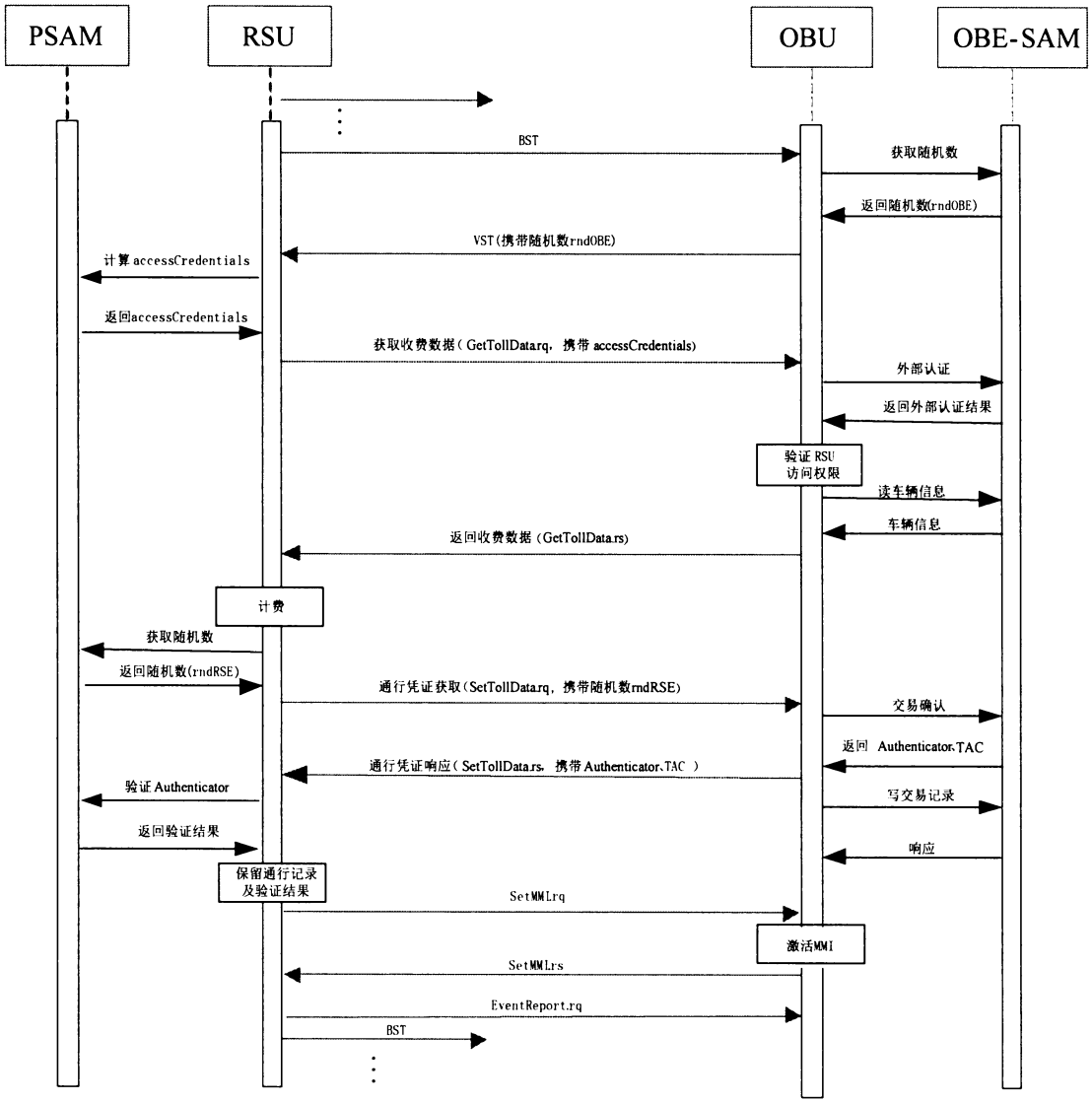


图 6-1 单片式 OBU 开放式自由流收费交易流程

6.2.2 通信链路建立及应用信息获取阶段

6.2.2.1 概述

该阶段主要完成通信链路的建立，协商通信参数，协商应用参数，可获取部分应用信息等。其过程如下：

——RSU：BST；

——OBU：VST。

6.2.2.2 BST

6.2.2.2.1 简要说明

LLC 层使用 UI 命令。

APP 层使用 Initialization.request，T-APDUs=Initialization-Request=BST。

6.2.2.2.2 数据定义

BST 的 ASN.1 数据结构说明如下：

```
BST::=SEQUENCE{
    fillBIT                 BIT STRING(SIZE(3)),
    rsu                     BeaconID,
    time                    Time,
    profile                 Profile,
    mandapplications        ApplicationList,
    nonmandapplications     ApplicationList OPTIONAL,
    profileList             SEQUENCE(SIZE（0..127,...)) OF Profile
    }
```

其编码规定如下：

——无 nonmandapplications 数据元；

——BST 中的 BeaconID 为 RSU 设备 ID，见 GB/T 20851.3 规定；

——ApplicationList 为一个应用，aid=1，无 did；

——profileList 为无扩展，0 个 Profile，其编码为“0000 0000”。

根据实际应用场景需求，可预读或通过 GetTollData.request 原语获取收费公

路 ETC 应用入 / 出口信息文件 EF02。若采用预读方式，参见《收费公路联网电子不停车收费技术要求》（交通运输部 2011 年第 13 号公告）规定，复用参数 pretreat0019。

6.2.2.3 **VST**

6.2.2.3.1 简要说明

LLC 层使用 UI 命令。

APP 层使用 Initialization.response，T-APDUs=Initialization-Response=VST。

6.2.2.3.2 数据定义

VST 的 ASN.1 数据结构说明如下:

```
VST::=SEQUENCE{
    fillBIT              BIT    STRING (SIZE(4)),
    profile              Profile,
    applications         ApplicationList,
    obeConfiguration     OBEConfiguration
    }
```

其中 ApplicationList 的 applicationParameter 定义应符合 GB/T20851.4 的规定，rndOBE 应存在，由 OBU 通过 OBE-SAM 获取，参见附录 C.3。

```
OBUConfiguration::=SEQUENCE{
    macID              INTEGER(0..4294967295),-- MAC 地址
    equipmentClass     BIT STRING (SIZE(4)),-- 0100₂ 单片式 OBU
    equipmentVersion BIT STRING (SIZE(4)),
    obuStatus          OBUStatus
    }
```

其中 equipmentClass 取值为 0100_2。

6.2.3 收费数据获取阶段

6.2.3.1 **概述**

读取 OBE-SAM 内的车辆信息，其过程如下：

——RSU：GetTollData.request；

——OBU：GetTollData.response。

RSU 使用 GetTollData.request 服务原语应携带 accessCredentials，实现对 OBU 访问许可认证。

6.2.3.2 **GetTollData.request**

6.2.3.2.1 简要说明

LLC 层使用 ACn 命令。

APP 层使用 Action.request，T-APDUs= Action-Request。

GetTollData.request 原语应携带访问证书（AccessCredentials），用于获得读取 OBU 中数据的权限，实现 OBU 对 RSU 的单方向认证。

6.2.3.2.2 数据定义

GetTollData.request 的 ASN.1 数据结构说明如下:

```
Action-Request::=SEQUENCE{
    mode              BOOLEAN,
    did               Dsrc-DID,
    actionType        ActionType,
    accessCredentials  OCTET STRING (SIZE(0..127,...)) OPTIONAL,
    actionParameter   Container OPTIONAL,
    iid               Dsrc-DID OPTIONAL
    }
```

其编码规定如下：

——mode：采用确认模式，取值为 1；

——Dsrc-DID::=INTEGER(0..127,...) 无扩展，ETC 应用目录号为 1，取值 1；

——ActionType::=INTEGER(0..127,...) 无扩展，取值 5；

——accessCredentials OCTET STRING (SIZE(0..127,...)) 无扩展，应存在，Length 为 8，取值 8，accessCredentials 的取值为 8 字节。accessCredentials 为 RSU 计算得到的访问证书，可用于 accessCredentials 计算的随机数 rndOBE 可从 6.2.2.3 所述的 VST 中获得，accessCredentials 数据由 RSU 通过 PSAM 获取。

actionParameter 为 Container 类型，Container.Type=42（GetTollDataRq），在

公路 ETC 应用中应存在。

GetTollDataRq 的 ASN.1 数据结构说明如下:

```
GetTollDataRq::=SEQUENCE{
    fillBIT          BIT    STRING (SIZE(4)),
    transType        OCTET STRING (SIZE(1)),
    vehicleInfo      RangeOfFile,
    tollInfo          RangeOfFile OPTIONAL,
    rndRSE            Rand    OPTIONAL,
    keyIdForAC        INTEGER(0..255) OPTIONAL,
    keyIdForAuthen    INTEGER(0..255) OPTIONAL
    }
```

其中 RangeOfFile 的 ASN.1 数据结构说明如下:

```
RangeOfFile::=SEQUENCE{
    offset    INTEGER(0.. 32767,...),
    length    INTEGER(0..127,...)
    }
```

vehicleInfo　RangeOfFile, 其中：

——offset　INTEGER(0..32767,...)，无扩展，取值等于读取 ETC 应用车辆信息文件实际的偏移量；

——length　INTEGER(0..127,...)，无扩展，取值等于读取 ETC 应用车辆信息文件的实际长度。

transType　OCTET STRING (SIZE(1))，交易类型，取值参见附录 C.12。

tollInfo　RangeOfFile OPTIONAL，可选项，根据实际应用需求确定是否存在。

rndRSE　Rand　OPTIONAL，可选项，本应用场景不存在。

keyIdForAC　INTEGER(0..255) OPTIONAL，用于指示访问许可使用的密钥标识，提供 OBU 选择相应的密钥进行访问许可认证。

keyIdForAuthen　INTEGER(0..255) OPTIONAL，可选项，本应用场景不存在。

公路 ETC 应用中不存在 iid 数据元。

6.2.3.3 GetTollData.response

6.2.3.3.1 简要说明

LLC 层使用 ACn 响应。

APP 层使用 Action.response，T-APDUs= Action-Response。

GetTollData.response 返回读取文件内容。

6.2.3.3.2 数据定义

GetTollData.response 的 ASN.1 数据结构说明如下:

```
Action-Response::=SEQUENCE{
    fill                BIT STRING (SIZE(2)),
    did                 Dsrc-DID,
    responseParameter   Container OPTIONAL,
    iid                 Dsrc-DID OPTIONAL,
    ret                 ReturnStatus
    }
```

其编码规定如下：

——did，取值 1；

——responseParameter 为 Container 类型，Container.Type=43（GetTollDataRs）。

OBU 通过 OBE-SAM 使用指令（指令参见附录 C.2）来验证 RSU 是否具备访问权限并通过 ret 指示访问权限验证结果，ret 定义应符合 GB / T 20851.3 附录 A 的规定。当 ret = 0x00 时，responseParameter 应存在，ret 为其他取值时 responseParameter 不存在。

GetTollDataRs 的 ASN.1 数据格式说明如下：

```
GetTollDataRs::=SEQUENCE {
  fillBIT         BIT   STRING (SIZE(6)),
  vehicleInfo     File,
  tollInfo        File    OPTIONAL,
  authenticator   OCTET STRING(SIZE(8))   OPTIONAL
```

}

其编码规定如下：

——vehicleInfo，File，读取 ETC 应用车辆信息文件内容；

——tollInfo，File　OPTIONAL，可选项；

——authenticator OCTET STRING(SIZE(8))　OPTIONAL 不存在。

在公路 ETC 应用中不存在 iid 数据元。

6.2.4 通行凭证

6.2.4.1 概述

使用 SetTollData 获取用户通行凭证 TAC 码。

其过程如下：

——RSU：SetTollData.request；

——OBU：SetTollData.response。

6.2.4.2 SetTollData.request

6.2.4.2.1 简要说明

LLC 层使用 ACn 命令。

APP 层使用 Action.request，T-APDUs= Action-Request。

SetTollData.request 原语请求 OBU 返回通行凭证。

6.2.4.2.2 数据定义

SetTollData.request 的 ASN.1 数据结构说明如下:

```
Action-Request::=SEQUENCE{
    mode                BOOLEAN,
    did                 Dsrc-DID,
    actionType          ActionType,
    accessCredentials   OCTET STRING (SIZE(0..127,...)) OPTIONAL,
    actionParameter     Container OPTIONAL,
    iid                 Dsrc-DID OPTIONAL
    }
```

其编码规定如下：

——mode：采用确认模式，取值为 1；

——did：取值 1；

——ActionType：无扩展，取值 6；

——accessCredentials：无扩展，不存在；

——actionParameter：Container.Type=44（SetTollDataRq），应存在。

SetTollDataRq 的 ASN.1 数据结构如下：

```
SetTollDataRq::=SEQUENCE{
    fillBIT             BIT    STRING (SIZE(6)),
    rndRSE              Rand,
    tacPara            TacPara,
    tollInfo           PartOfFile OPTIONAL,
    keyIdForAC      INTEGER(0..255) OPTIONAL,
    keyIdForAuthen INTEGER(0..255)
  }
```

其中 rndRSE Rand，由 RSU 通过 PSAM 获取。

tacPara　TacPara，其中 TAC 码计算参数的 ASN.1 类型定义为：

```
TacPara::=SEQUENCE{
    transAmount     OCTET STRING (SIZE(4)),--通行费额
    transType       OCTET STRING (SIZE(1)),--交易类型
    terminalID      OCTET STRING (SIZE(6)),--终端编号
    transSN         OCTET  STRING (SIZE(4)),--终端交易序号
    transTime       OCTET STRING (SIZE(7)),--通行时间
    transStationID  OCTET STRING (SIZE(3)) –ETC 门架编号 / 收费站编号
    }
```

tollInfo　　PartOfFile OPTIONAL，本应用场景不存在。

keyIdForAC　INTEGER(0..255) OPTIONAL，本应用场景不存在。

keyIdForAuthen INTEGER(0..255)，用于指示信息鉴别使用的密钥版本，提供 OBU 选择相应的密钥进行对返回信息进行信息鉴别计算，计算方法参见 GB/T 20851.4 中“8.3 信息鉴别”。

在公路 ETC 应用中不存在 iid 数据元。

6.2.4.3 SetTollData.response

6.2.4.3.1 简要说明

LLC 层使用 ACn 响应。

APP 层使用 Action.response，T-APDUs= Action-Response。

在本应用中，SetTollData.response 原语应携带 OBU 使用指定密钥计算得到的鉴别报文（authenticator），在保护 DSRC 传输过程中的数据完整性的同时，也让 RSU 完成对 OBU 合法性的单方向认证，同时返回通行凭证 TAC 码。

6.2.4.3.2 数据定义

SetTollData.response 的 ASN.1 数据结构说明如下：

```
Action-Response::=SEQUENCE{
    fillBIT                BIT   STRING (SIZE(2)),
    did                    Dsrc-DID,
    responseParameter      Container OPTIONAL,
    iid                    Dsrc-DID OPTIONAL,
    ret                    ReturnStatus
    }
```

其编码规定如下：

——did，无扩展，取值 1；

——responseParameterContainer.Type=45（SetTollDataRs），当 ret=0 应存在。

SetTollDataRs 的 ASN.1 数据结构如下：

```
SetTollDataRs::=SEQUENCE{
    tacInfo          OCTET STRING (SIZE(4)),
    authenticator    OCTET STRING (SIZE(8))
    }
```

OBU 计算 tacInfo 和 authenticator 使用指令参见附录 C.12。

在公路 ETC 应用中不存在 iid 数据元。

OBU 在返回 SetTollData.response 后，应将交易记录写入 OBE-SAM 的 DF01

/ EF04 中，使用指令参见附录 C.10。

6.2.5 用户提示

6.2.5.1 概述

提示用户交易结果。其过程如下：

——RSU：SetMMI.request；

——OBU：SetMMI.response。

6.2.5.2 SetMMI.request

6.2.5.2.1 简要说明

LLC层使用ACn命令。

APP层使用Action.request，T-APDUs= Action-Request。

本应用中，SetMMI中无需accessCredentials。

6.2.5.2.2 数据定义

SetMMI.request的ASN.1数据结构说明如下：

```
Action-Request::=SEQUENCE{
    mode                BOOLEAN,
    did                 Dsrc-DID,
    actionType          ActionType,
    accessCredentials   OCTET STRING (SIZE(0..127,...)) OPTIONAL,
    actionParameter     Container OPTIONAL,
    iid                 Dsrc-DID OPTIONAL
    }
```

其编码规定如下：

——mode：采用确认模式，取值为1；

——did：无扩展，取值为1；

——ActionType：无扩展，取值为4；

——accessCredentials：无扩展，可选性使用；

——actionParameter：Container.Type=26（SetMMIRq），应存在。

6.2.5.3 SetMMI.response

6.2.5.3.1 简要说明

LLC层使用ACn响应。

APP层使用Action.response，T-APDUs= Action-Response。

6.2.5.3.2 数据定义

SetMMI.response的ASN.1数据结构说明如下：

```
Action-Response::=SEQUENCE{
    fill                BIT STRING (SIZE(2)),
    did                 Dsrc-DID,
    responseParameter   Container OPTIONAL,
    iid                 Dsrc-DID OPTIONAL,
    ret                 ReturnStatus
    }
```

其编码规定如下：

——did，无扩展，取值为1；

——responseParameter应不存在；

——iid应不存在。

6.2.6 链路释放

6.2.6.1 概述

RSU 释放与 OBU 的通信连接。

RSU：Event-Report(Release)。

6.2.6.2 Event-Report(Release)

6.2.6.2.1 简要说明

LLC层使用UI命令，无需响应。

APP层使用Action.request，T-APDUs= event-report-request。

Event-Report(Release)用于释放OBU，让OBU进入休眠状态。

6.2.6.2.2 数据定义

```
Event-Report-Request::=SEQUENCE{
    mode                BOOLEAN,
    did                 DirectoryID,
    eventType           EventType,
    accessCredentials   OCTET STRING (SIZE(0..127,...)) OPTIONAL,
    eventParameter      Container OPTIONAL,
    iid                 Dsrc-DID OPTIONAL
    }
```

其编码规定如下：

——mode：采用非确认模式，取值为0；

——did：无扩展，因为Event-Report与应用无关，应取值为系统（OBU）=0；

——accessCredentials：无扩展，可选性使用；

——eventParameter：不存在；

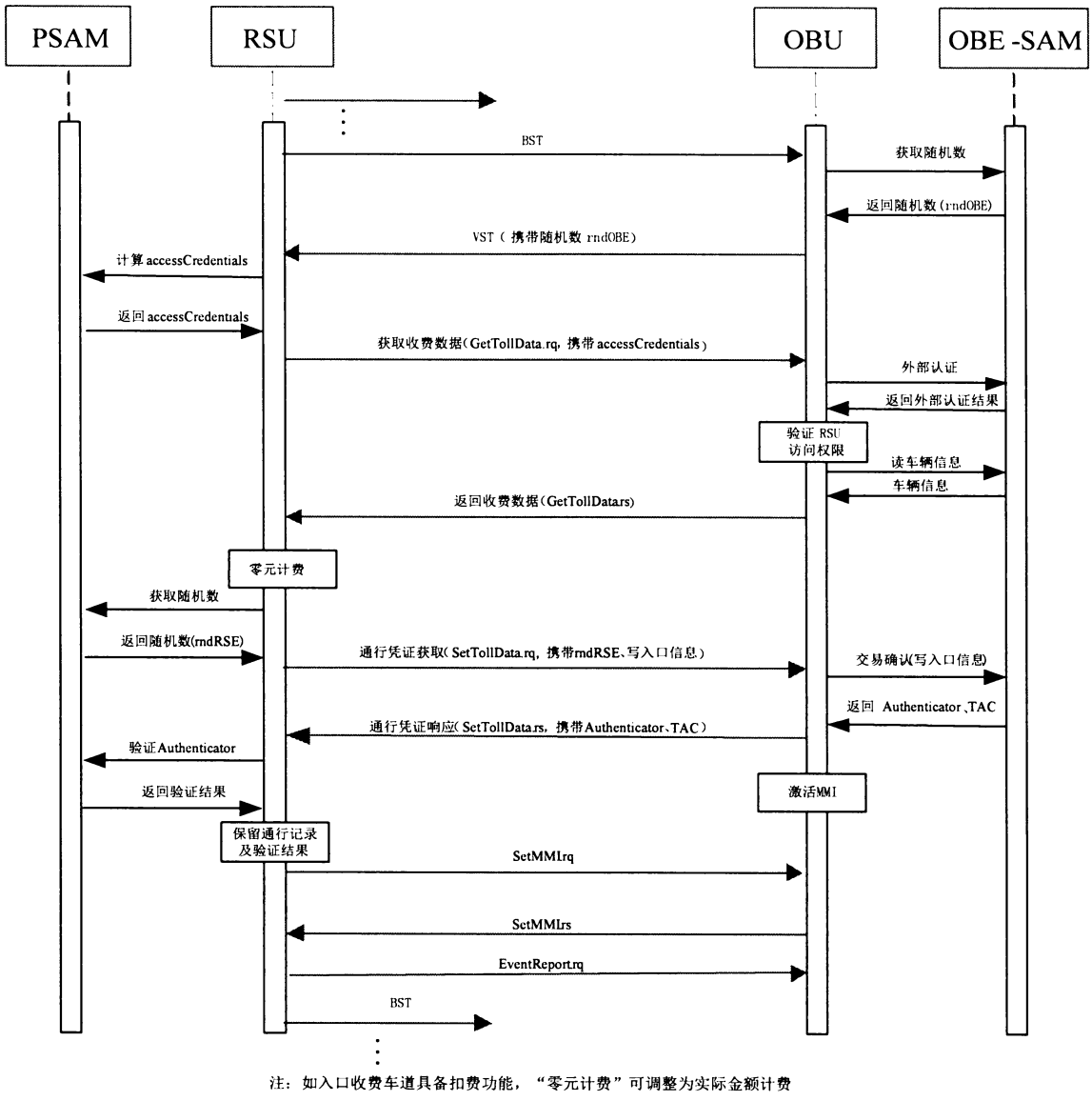
——eventType：EventType。

6.3 封闭式交易流程

6.3.1 封闭式入口交易流程

6.3.1.1 交易流程框架

封闭式入口交易流程划分为通信链路建立、收费数据（车辆信息）获取、通行凭证及入口信息写入、用户提示和链路释放五个主要阶段，其交易流程如图6-2所示。



注：如入口收费车道具备扣费功能，“零元计费”可调整为实际金额计费

图 6-2 单片式 OBU 封闭式入口交易流程

6.3.1.2 通信链路建立及应用信息获取阶段

6.3.1.2.1 概述

该阶段主要完成通信链路的建立，协商通信参数，协商应用参数，可获取部分应用信息等。其过程如下：

——RSU：BST；

——OBU：VST。

6.3.1.2.2 BST

6.3.1.2.2.1 简要说明

LLC 层使用 UI 命令。

APP 层使用 Initialization.request，T-APDUs=Initialization-Request=BST。

6.3.1.2.2.2 数据定义

BST 的 ASN.1 数据结构说明如下：

```
BST::=SEQUENCE{
    fillBIT                 BIT   STRING(SIZE(3)),
    rsu                     BeaconID,
    time                    Time,
    profile                 Profile,
    mandapplications        ApplicationList,
    nonmandapplications     ApplicationList OPTIONAL,
    profileList             SEQUENCE(SIZE（0..127,...)) OF Profile
    }
```

其编码规定如下：

——无 nonmandapplications 数据元；

——BST 中的 BeaconID 为 RSU 设备 ID，见 GB/T 20851.3 规定；

——ApplicationList 为一个应用，aid=1，无 did；

——profileList 为无扩展，0 个 Profile，其编码为“0000 0000”。

6.3.1.2.3 VST

6.3.1.2.3.1 简要说明

LLC 层使用 UI 命令。

APP 层使用 Initialization.response，T-APDUs=Initialization-Response=VST。

6.3.1.2.3.2 数据定义

VST 的 ASN.1 数据结构说明如下:

```
VST::=SEQUENCE{
    fillBIT              BIT STRING (SIZE(4)),
    profile              Profile,
    applications         ApplicationList,
    obeConfiguration     OBEConfiguration
    }
```

其中 ApplicationList 的 applicationParameter 定义应符合 GB/T20851.4 的规定，rndOBE 应存在，由 OBU 通过 OBE-SAM 获取，参见附录 C.3。

```
OBUConfiguration::=SEQUENCE{
  macID              INTEGER(0..4294967295),-- MAC 地址
  equipmentClass     BIT STRING (SIZE(4)),-- 0100₂ 单片式 OBU
  equipmentVersion   BIT STRING (SIZE(4)),
  obuStatus          OBUStatus
  }
```

其中 equipmentClass 取值为 0100_2。

6.3.1.3 收费数据获取阶段

6.3.1.3.1 概述

读取 OBE-SAM 内的车辆信息，其过程如下：

——RSU：GetTollData.request；

——OBU：GetTollData.response。

RSU 使用 GetTollData.request 服务原语应携带 accessCredentials，实现对 OBU 访问许可认证。

6.3.1.3.2 GetTollData.request

6.3.1.3.2.1 简要说明

LLC 层使用 ACn 命令。

APP 层使用 Action.request，T-APDUs= Action-Request。

GetTollData.request 原语应携带访问证书（AccessCredentials），用于获得读取 OBU 中数据的权限，实现 OBU 对 RSU 的单方向认证。

6.3.1.3.2.2 数据定义

GetTollData.request 的 ASN.1 数据结构说明如下:

```
Action-Request::=SEQUENCE{
    mode              BOOLEAN,
    did               Dsrc-DID,
    actionType        ActionType,
    accessCredentials  OCTET STRING (SIZE(0..127,...)) OPTIONAL,
    actionParameter    Container OPTIONAL,
    iid               Dsrc-DID OPTIONAL
    }
```

其编码规定如下：

——mode：采用确认模式，取值为 1；

——Dsrc-DID::=INTEGER(0..127,...) 无扩展，ETC 应用目录号为 1，取值 1；

——ActionType::=INTEGER(0..127,...) 无扩展，取值 5；

——accessCredentials OCTET STRING (SIZE(0..127,...)) 无扩展，应存在，Length 为 8，取值 8，accessCredentials 的取值为 8 字节。accessCredentials 为 RSU 计算得到的访问证书，可用于 accessCredentials 计算的随机数 rndOBE 可从 6.3.1.2.3 所述的 VST 中获得，accessCredentials 数据由 RSU 通过 PSAM 获取。

actionParameter 为 Container 类型，Container.Type=42（GetTollDataRq），在公路 ETC 应用中应存在。

GetTollDataRq 的 ASN.1 数据结构说明如下:

```
GetTollDataRq::=SEQUENCE{
    fillBIT           BIT   STRING (SIZE(5)),
    transType         OCTET STRING (SIZE(1)),
    vehicleInfo       RangeOfFile,
    tollInfo          RangeOfFile OPTIONAL,
    rndRSE            Rand   OPTIONAL,
    keyIdForAC        INTEGER(0..255) OPTIONAL,
    keyIdForAuthen    INTEGER(0..255) OPTIONAL
```

}

其中 RangeOfFile 的 ASN.1 数据结构说明如下:

RangeOfFile::=SEQUENCE{

offset INTEGER(0.. 32767,...),

length INTEGER(0..127,...)

}

vehicleInfo RangeOfFile, 其中:

——offset INTEGER(0..32767,...)，无扩展，取值等于读取 ETC 应用车辆信息文件实际的偏移量;

——length INTEGER(0..127,...)，无扩展，取值等于读取 ETC 应用车辆信息文件的实际长度。

transType OCTET STRING (SIZE(1))，交易类型，取值参见附录 C.12。

tollInfo RangeOfFile OPTIONAL，可选项。

rndRSE Rand OPTIONAL，可选项，本应用场景不存在。

keyIdForAC INTEGER(0..255) OPTIONAL，用于指示访问许可使用的密钥标识，提供 OBU 选择相应的密钥进行访问许可认证。

keyIdForAuthen INTEGER(0..255) OPTIONAL，可选项，本应用场景不存在。

公路 ETC 应用中不存在 iid 数据元。

6.3.1.3.3 GetTollData.response

6.3.1.3.3.1 简要说明

LLC 层使用 ACn 响应。

APP 层使用 Action.response，T-APDUs= Action-Response。

GetTollData.response 返回读取文件内容。

6.3.1.3.3.2 数据定义

GetTollData.response 的 ASN.1 数据结构说明如下:

Action-Response::=SEQUENCE{

```
    fill                BIT STRING (SIZE(2)),
    did                 Dsrc-DID,
    responseParameter   Container OPTIONAL,
    iid                 Dsrc-DID OPTIONAL,
    ret                 ReturnStatus
    }
```

其编码规定如下：

——did，取值 1；

——responseParameter 为 Container 类型，Container.Type=43（GetTollDataRs）。

OBU 通过 OBE-SAM 指令（指令参见附录 C.2）来验证 RSU 是否具备访问权限并通过 ret 指示访问权限验证结果，ret 定义应符合 GB / T 20851.3 附录 A 的规定。当 ret = 0x00 时，responseParameter 应存在，ret 为其他取值时 responseParameter 不存在。

GetTollDataRs 的 ASN.1 数据格式说明如下：

```
GetTollDataRs::=SEQUENCE {
    fillBIT         BIT   STRING (SIZE(6)),
    vehicleInfo     File,
    tollInfo        File   OPTIONAL,
    authenticator   OCTET STRING(SIZE(8))   OPTIONAL
    }
```

其编码规定如下：

——vehicleInfo，File，读取 ETC 应用车辆信息文件内容；

——tollInfo，File　OPTIONAL，可选项；

——authenticator OCTET STRING(SIZE(8)) OPTIONAL 本应用场景不存在。

在公路 ETC 应用中不存在 iid 数据元。

6.3.1.4 通行凭证及入口信息写入

6.3.1.4.1 概述

使用 SetTollData 写入入口信息并获取用户通行凭证 TAC 码。

其过程如下：

——RSU：SetTollData.request；

——OBU：SetTollData.response。

6.3.1.4.2 SetTollData.request

6.3.1.4.2.1 简要说明

LLC 层使用 ACn 命令。

APP 层使用 Action.request，T-APDUs= Action-Request。

SetTollData.request 原语写入入口信息并请求 OBU 返回通行凭证 TAC 码。

6.3.1.4.2.2 数据定义

SetTollData.request 的 ASN.1 数据结构说明如下:

```
Action-Request::=SEQUENCE{
    mode                BOOLEAN,
    did                 Dsrc-DID,
    actionType          ActionType,
    accessCredentials   OCTET STRING (SIZE(0..127,...)) OPTIONAL,
    actionParameter     Container OPTIONAL,
    iid                 Dsrc-DID OPTIONAL
    }
```

其编码规定如下：

——mode：采用确认模式，取值为 1；

——did：取值 1；

——ActionType：无扩展，取值 6；

——accessCredentials：无扩展，不存在；

——actionParameter：Container.Type=44（SetTollDataRq），应存在。

SetTollDataRq 的 ASN.1 数据结构如下：

```
SetTollDataRq::=SEQUENCE{
    fillBIT             BIT STRING (SIZE(6)),
    rndRSE              Rand,
    tacPara             TacPara,
    tollInfo            PartOfFile OPTIONAL,
    keyIdForAC          INTEGER(0..255) OPTIONAL,
    keyIdForAuthen      INTEGER(0..255)
    }
```

其中 rndRSE Rand，由 RSU 通过 PSAM 获取。

tacPara　TacPara。其中 TAC 码计算参数的 ASN.1 类型定义为：

```
TacPara::=SEQUENCE{
    transAmount     OCTET STRING (SIZE(4)),--通行费额
    transType       OCTET STRING (SIZE(1)),--交易类型
    terminalID      OCTET STRING (SIZE(6)),--终端编号
    transSN         OCTET  STRING (SIZE(4)),--终端交易序号
    transTime       OCTET STRING (SIZE(7))，--通行时间
    transStationID  OCTET STRING (SIZE(3)) --ETC 门架编号 / 收费站编号
    }
```

tollInfo　PartOfFile OPTIONAL，本应用场景应存在。

其 PartOfFile 的 ASN.1 类型定义为：

```
PartOfFile::=SEQUENCE{
    offset              INTEGER(0..32767,...),
    length              INTEGER(0..127,...),
    fileContent         File
    }
```

其中：

——offset　INTEGER(0..32767,...)，无扩展，取值等于写入 / 出口信息文件实际的偏移量；

——length　INTEGER(0..127,...)，无扩展，取值等于写入 / 出口信息文件实际的长度。

——fileContent　File，写入 / 出口信息文件实际的内容。

keyIdForAC　INTEGER(0..255) OPTIONAL，本应用场景不存在。

keyIdForAuthen INTEGER(0..255) ，用于指示信息鉴别使用的密钥版本，提供 OBU 选择相应的密钥进行对返回信息进行信息鉴别计算，计算方法参见 GB/T 20851.4 中“8.3 信息鉴别”。

在公路 ETC 应用中不存在 iid 数据元。

6.3.1.4.3 SetTollData.response

6.3.1.4.3.1 简要说明

LLC 层使用 ACn 响应。

APP 层使用 Action.response，T-APDUs= Action-Response。

在本应用中，SetTollData.response 原语应携带 OBU 使用指定密钥计算得到的鉴别报文（authenticator），在保护 DSRC 传输过程中的数据完整性的同时，也让 RSU 完成对 OBU 合法性的单方向认证，同时返回通行凭证 TAC 码。

6.3.1.4.3.2 数据定义

SetTollData.response 的 ASN.1 数据结构说明如下：

```
Action-Response::=SEQUENCE{
    fillBIT                 BIT    STRING (SIZE(2)),
    did                     Dsrc-DID,
    responseParameter       Container OPTIONAL,
    iid                     Dsrc-DID OPTIONAL,
    ret                     ReturnStatus
    }
```

其编码规定如下：

——did，无扩展，取值 1；

——responseParameterContainer.Type=45（SetTollDataRs），当 ret=0 应存在。

SetTollDataRs 的 ASN.1 数据结构如下：

```
SetTollDataRs::=SEQUENCE{
    tacInfo          OCTET STRING (SIZE(4)),
    authenticator    OCTET STRING (SIZE(8))
  }
```

OBU 计算 tacInfo 和 authenticator 使用指令参见附录 C.12。

在公路 ETC 应用中不存在 iid 数据元。

6.3.1.5 用户提示

6.3.1.5.1 概述

提示用户交易结果。其过程如下：

——RSU：SetMMI.request；

——OBU：SetMMI.response。

6.3.1.5.2 SetMMI.request

6.3.1.5.2.1 简要说明

LLC层使用ACn命令。

APP层使用Action.request，T-APDUs= Action-Request。

本应用中，SetMMI中无需accessCredentials。

6.3.1.5.2.2 数据定义

SetMMI.request的ASN.1数据结构说明如下：

```
Action-Request::=SEQUENCE{
    mode                BOOLEAN,
    did                 Dsrc-DID,
    actionType          ActionType,
    accessCredentials   OCTET STRING (SIZE(0..127,...)) OPTIONAL,
    actionParameter     Container OPTIONAL,
    iid                 Dsrc-DID OPTIONAL
    }
```

其编码规定如下：

——mode：采用确认模式，取值为1；

——did：无扩展，取值为1；

——ActionType：无扩展，取值为4；

——accessCredentials：无扩展，可选性使用；

——actionParameter：Container.Type=26（SetMMIRq），应存在。

6.3.1.5.3 SetMMI.response

6.3.1.5.3.1 简要说明

LLC层使用ACn响应。

APP层使用Action.response，T-APDUs= Action-Response。

6.3.1.5.3.2 数据定义

SetMMI.response的ASN.1数据结构说明如下：

```
Action-Response::=SEQUENCE{
    fill                    BIT STRING (SIZE(2)),
    did                     Dsrc-DID,
    responseParameter       Container OPTIONAL,
    iid                     Dsrc-DID OPTIONAL,
    ret                     ReturnStatus
    }
```

其编码规定如下：

——did，无扩展，取值为1；

——responseParameter应不存在；

——iid应不存在。

6.3.1.6 链路释放

6.3.1.6.1 概述

RSU 释放与 OBU 的通信连接。

RSU：Event-Report(Release)。

6.3.1.6.2 Event-Report(Release)

6.3.1.6.2.1 简要说明

LLC层使用UI命令，无需响应。

APP层使用Action.request，T-APDUs= event-report-request。

Event-Report(Release)用于释放OBU，让OBU进入休眠状态。

6.3.1.6.2.2 数据定义

```
Event-Report-Request::=SEQUENCE{
    mode              BOOLEAN,
    did               DirectoryID,
    eventType         EventType,
    accessCredentials OCTET STRING (SIZE(0..127,...)) OPTIONAL,
    eventParameter    Container OPTIONAL,
    iid               Dsrc-DID OPTIONAL
    }
```

其编码规定如下：

——mode：采用非确认模式，取值为0；

——did：无扩展，因为Event-Report与应用无关，应取值为系统（OBU）=0；

——accessCredentials：无扩展，可选性使用；

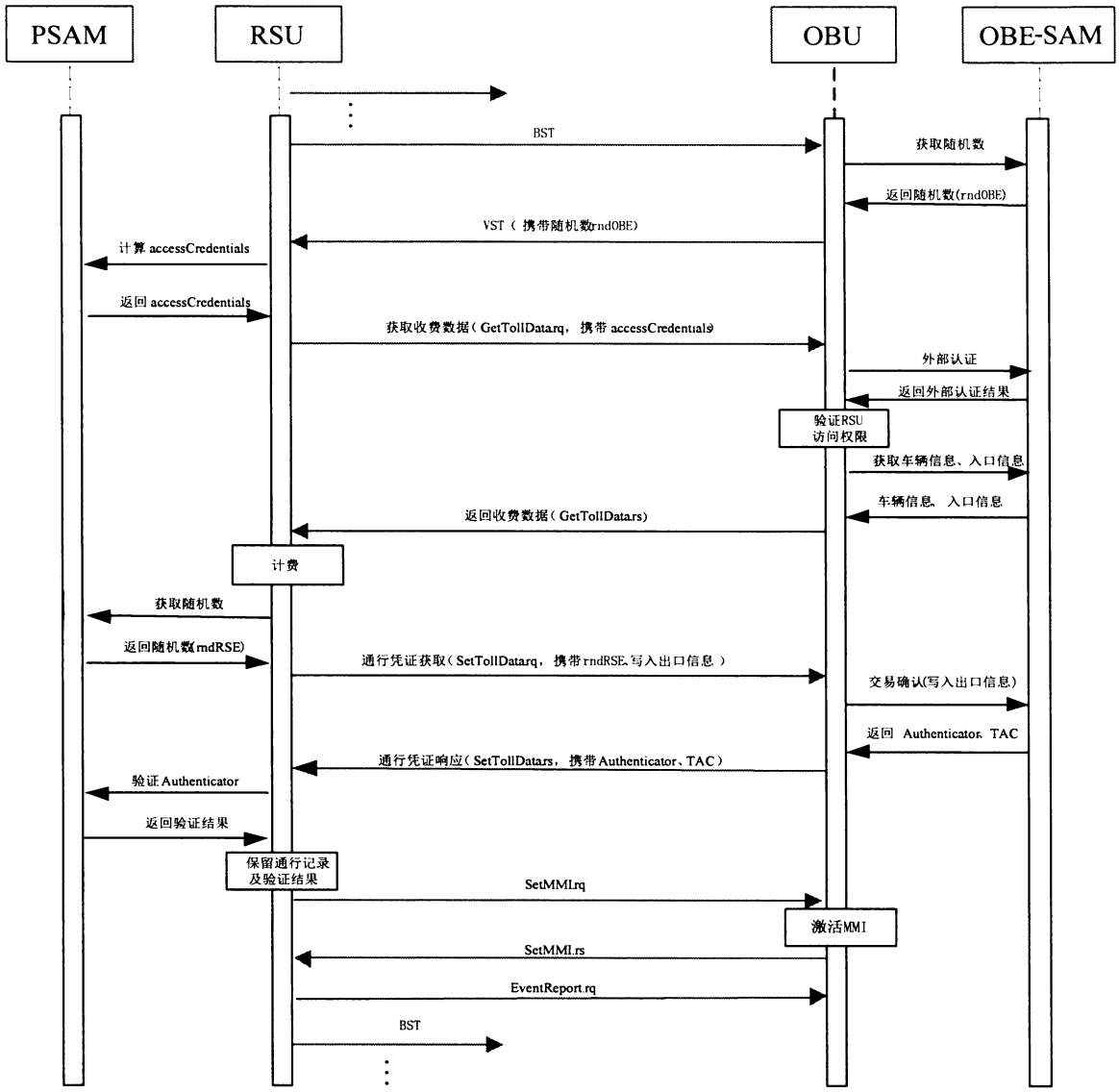
——eventParameter：不存在；

——eventType：EventType。

6.3.2 封闭式出口交易流程

6.3.2.1 交易流程框架

封闭式出口交易流程划分为通信链路建立、收费数据（车辆信息和入口信息）获取、通行凭证及出口信息写入、用户提示和链路释放五个主要阶段，其交易流程如图 6-3 所示。



注：当车道系统无计费功能时，“计费”功能可为零元计费

图 6-3 单片式 OBU 封闭式出口交易流程

6.3.2.2 通信链路建立及应用信息获取阶段

6.3.2.2.1 概述

该阶段主要完成通信链路的建立，协商通信参数，协商应用参数，可获取部分应用信息等。其过程如下：

——RSU：BST；

——OBU：VST。

6.3.2.2.2 BST

6.3.2.2.2.1 简要说明

LLC 层使用 UI 命令。

APP 层使用 Initialization.request，T-APDUs=Initialization-Request=BST。

6.3.2.2.2.2 数据定义

BST 的 ASN.1 数据结构说明如下：

```
BST::=SEQUENCE{
    fillBIT                 BIT   STRING(SIZE(3)),
    rsu                     BeaconID,
    time                    Time,
    profile                 Profile,
    mandapplications        ApplicationList,
    nonmandapplications     ApplicationList OPTIONAL,
    profileList             SEQUENCE(SIZE（0..127,...)) OF Profile
    }
```

其编码规定如下：

——无 nonmandapplications 数据元；

——BST 中的 BeaconID 为 RSU 设备 ID，见 GB/T 20851.3 规定；

——ApplicationList 为一个应用，aid=1，无 did；

——profileList 为无扩展，0 个 Profile，其编码为“0000 0000”。

6.3.2.2.3 VST

6.3.2.2.3.1 简要说明

LLC 层使用 UI 命令。

APP 层使用 Initialization.response，T-APDUs=Initialization-Response=VST。

6.3.2.2.3.2 数据定义

VST 的 ASN.1 数据结构说明如下:

```
VST::=SEQUENCE{
    fillBIT              BIT   STRING (SIZE(4)),
    profile              Profile,
    applications         ApplicationList,
    obeConfiguration     OBEConfiguration
    }
```

其中 ApplicationList 的 applicationParameter 定义应符合 GB/T20851.4 的规定，rndOBE 应存在，由 OBU 通过 OBE-SAM 获取，参见附录 C.3。

```
OBUConfiguration::=SEQUENCE{
  macID              INTEGER(0..4294967295),-- MAC 地址
  equipmentClass     BIT STRING (SIZE(4)),-- 0100₂ 单片式 OBU
  equipmentVersion   BIT STRING (SIZE(4)),
  obuStatus          OBUStatus
  }
```

其中 equipmentClass 取值为 0100_2。

6.3.2.3 收费数据获取阶段

6.3.2.3.1 概述

读取 OBE-SAM 内的车辆信息和入口信息，其过程如下：

——RSU：GetTollData.request；

——OBU：GetTollData.response。

RSU 使用 GetTollData.request 服务原语应携带 accessCredentials，实现对 OBU 访问许可认证。

6.3.2.3.2 GetTollData.request

6.3.2.3.2.1 简要说明

LLC 层使用 ACn 命令。

APP 层使用 Action.request，T-APDUs= Action-Request。

GetTollData.request 原语应携带访问证书（AccessCredentials），用于获得读取 OBU 中数据的权限，实现 OBU 对 RSU 的单方向认证。

注：若读取信息超过协议数据帧规定的最大长度，RSU 可采用多次读取方式实现

6.3.2.3.2.2 数据定义

GetTollData.request 的 ASN.1 数据结构说明如下:

```
Action-Request::=SEQUENCE{
    mode              BOOLEAN,
    did               Dsrc-DID,
    actionType        ActionType,
    accessCredentials  OCTET STRING (SIZE(0..127,...)) OPTIONAL,
    actionParameter   Container OPTIONAL,
    iid               Dsrc-DID OPTIONAL
    }
```

其编码规定如下：

——mode：采用确认模式，取值为 1；

——Dsrc-DID::=INTEGER(0..127,...) 无扩展，ETC 应用目录号为 1，取值 1；

——ActionType::=INTEGER(0..127,...) 无扩展，取值 5；

——accessCredentials OCTET STRING (SIZE(0..127,...)) 无扩展，应存在，Length 为 8，取值 8，accessCredentials 的取值为 8 字节。accessCredentials 为 RSU 计算得到的访问证书，可用于 accessCredentials 计算的随机数 rndOBE 可从 6.3.2.2.3 所述的 VST 中获得，accessCredentials 数据由 RSU 通过 PSAM 获取。

actionParameter 为 Container 类型，Container.Type=42（GetTollDataRq），在公路 ETC 应用中应存在。

GetTollDataRq 的 ASN.1 数据结构说明如下:

```
GetTollDataRq::=SEQUENCE{
    fillBIT           BIT STRING (SIZE(5)),
    transType         OCTET STRING (SIZE(1)),
    vehicleInfo       RangeOfFile,
    tollInfo          RangeOfFile OPTIONAL,
    rndRSE            Rand  OPTIONAL,
    keyIdForAC        INTEGER(0..255) OPTIONAL,
```

keyIdForAuthen　INTEGER(0..255) OPTIONAL

}

其中 RangeOfFile 的 ASN.1 数据结构说明如下:

RangeOfFile::=SEQUENCE{

offset　INTEGER(0.. 32767,...),

length　INTEGER(0..127,...)

}

transType　OCTET STRING (SIZE(1))，交易类型，取值参见附录 C.12。

vehicleInfo　RangeOfFile, 其中：

——offset　INTEGER(0..32767,...)，无扩展，取值等于读取 ETC 应用车辆信息文件实际的偏移量；

——length　INTEGER(0..127,...)，无扩展，取值等于读取 ETC 应用车辆信息文件的实际长度。

tollInfo　RangeOfFile　OPTIONAL，可选项，本应用场景应存在，根据交易类型，确定写入入 / 出口信息文件。

——offset　INTEGER(0..32767,...)，无扩展，取值等于读取文件实际的偏移量；

——length　INTEGER(0..127,...)，无扩展，取值等于读取文件实际的长度。

rndRSE　Rand　OPTIONAL，可选项，本应用场景不存在。

keyIdForAC　INTEGER(0..255) OPTIONAL，用于指示访问许可使用的密钥标识，提供 OBU 选择相应的密钥进行访问许可认证。

keyIdForAuthen　INTEGER(0..255) OPTIONAL，可选项，本应用场景不存在。

公路 ETC 应用中不存在 iid 数据元。

6.3.2.3.3 GetTollData.response

6.3.2.3.3.1 简要说明

LLC 层使用 ACn 响应。

APP 层使用 Action.response，T-APDUs= Action-Response。

GetTollData.response 返回读取文件内容。

6.3.2.3.3.2 数据定义

GetTollData.response 的 ASN.1 数据结构说明如下:

```
Action-Response::=SEQUENCE{
    fill                BIT STRING (SIZE(2)),
    did                 Dsrc-DID,
    responseParameter   Container OPTIONAL,
    iid                 Dsrc-DID OPTIONAL,
    ret                 ReturnStatus
    }
```

其编码规定如下：

——did，取值 1；

——responseParameter 为 Container 类型，Container.Type=43（GetTollDataRs）。

OBU 通过 OBE-SAM 指令（指令参见附录 C.2）来验证 RSU 是否具备访问权限并通过 ret 指示访问权限验证结果，ret 定义应符合 GB / T 20851.3 附录 A 的规定。当 ret = 0x00 时，responseParameter 应存在，ret 为其他取值时 responseParameter 不存在。

GetTollDataRs 的 ASN.1 数据格式说明如下：

```
GetTollDataRs::=SEQUENCE {
    fillBIT         BIT   STRING (SIZE(6)),
    vehicleInfo     File,
    tollInfo        File   OPTIONAL,
    authenticator   OCTET STRING(SIZE(8))   OPTIONAL
    }
```

其编码规定如下：

——vehicleInfo，File，读取 ETC 应用车辆信息文件内容；

——tollInfo，File　OPTIONAL，本应用场景应存在，读取入 / 出口信息文

件内容；

——authenticator OCTET STRING(SIZE(8)) OPTIONAL 本应用场景不存在。

在公路 ETC 应用中不存在 iid 数据元。

6.3.2.4 通行凭证及出口信息写入

6.3.2.4.1 概述

使用 SetTollData 写入出口信息并获取用户通行凭证 TAC 码。

其过程如下：

——RSU：SetTollData.request；

——OBU：SetTollData.response。

6.3.2.4.2 SetTollData.request

6.3.2.4.2.1 简要说明

LLC 层使用 ACn 命令。

APP 层使用 Action.request，T-APDUs= Action-Request。

SetTollData.request 原语写入出口信息并请求 OBU 返回通行凭证 TAC 码。

6.3.2.4.2.2 数据定义

SetTollData.request 的 ASN.1 数据结构说明如下:

```
Action-Request::=SEQUENCE{
    mode              BOOLEAN,
    did               Dsrc-DID,
    actionType        ActionType,
    accessCredentials OCTET STRING (SIZE(0..127,...)) OPTIONAL,
    actionParameter   Container OPTIONAL,
    iid               Dsrc-DID OPTIONAL
    }
```

其编码规定如下：

——mode：采用确认模式，取值为 1；

——did：取值 1；

——ActionType：无扩展，取值 6；

——accessCredentials：无扩展，不存在；

——actionParameter：Container.Type=44（SetTollDataRq）,应存在。

SetTollDataRq 的 ASN.1 数据结构如下：

```
SetTollDataRq::=SEQUENCE{
    fillBIT             BIT STRING (SIZE(6)),
    rndRSE              Rand,
    tacPara             TacPara,
    tollInfo            PartOfFile OPTIONAL.
    keyIdForAC          INTEGER(0..255) OPTIONAL,
    keyIdForAuthen      INTEGER(0..255)
    }
```

其中 rndRSE Rand，由 RSU 通过 PSAM 获取。

tacPara　TacPara。其中 TAC 码计算参数的 ASN.1 类型定义为：

```
TacPara::=SEQUENCE{
    transAmount     OCTET STRING (SIZE(4)),--通行费额
    transType       OCTET STRING (SIZE(1)),--交易类型
    terminalID      OCTET STRING (SIZE(6)),--终端编号
    transSN         OCTET  STRING (SIZE(4)),--终端交易序号
    transTime       OCTET STRING (SIZE(7)),--通行时间
    transStationID  OCTET STRING (SIZE(3)) -- ETC 门架编号 / 收费站编
号
    }
```

tollInfo　PartOfFile OPTIONAL，本应用场景应存在。

其 PartOfFile 的 ASN.1 类型定义为：

```
PartOfFile::=SEQUENCE{
    offset              INTEGER(0..32767,...),
    length              INTEGER(0..127,...),
```

fileContent File

}

其中：

——offset INTEGER(0..32767,...)，无扩展，取值等于写入 / 出口信息文件实际的偏移量；

——length INTEGER(0..127,...)，无扩展，取值等于写入 / 出口信息文件实际的长度；

——fileContent File，写入 / 出口信息文件实际的内容。

keyIdForAC INTEGER(0..255) OPTIONAL，本应用场景不存在。

keyIdForAuthen INTEGER(0..255) ，用于指示信息鉴别使用的密钥版本，提供 OBU 选择相应的密钥进行对返回信息进行信息鉴别计算，计算方法参见 GB/T 20851.4 中“8.3 信息鉴别”。

在公路 ETC 应用中不存在 iid 数据元。

6.3.2.4.3 SetTollData.response

6.3.2.4.3.1 简要说明

LLC 层使用 ACn 响应。

APP 层使用 Action.response，T-APDUs= Action-Response。

在本应用中，SetTollData.response 原语应携带 OBU 使用指定密钥计算得到的鉴别报文（authenticator），在保护 DSRC 传输过程中的数据完整性的同时，也让 RSU 完成对 OBU 合法性的单方向认证，同时返回通行凭证 TAC 码。

6.3.2.4.3.2 数据定义

SetTollData.response 的 ASN.1 数据结构说明如下：

```
Action-Response::=SEQUENCE{
    fillBIT                 BIT   STRING (SIZE(2)),
    did                     Dsrc-DID,
    responseParameter       Container OPTIONAL,
    iid                     Dsrc-DID OPTIONAL,
```

ret ReturnStatus

}

其编码规定如下：

——did，无扩展，取值 1；

——responseParameterContainer.Type=45（SetTollDataRs），当 ret=0 应存在。

SetTollDataRs 的 ASN.1 数据结构如下：

SetTollDataRs::=SEQUENCE{

tacInfo OCTET STRING (SIZE(4)),

authenticator OCTET STRING (SIZE(8))

}

OBU 计算 tacInfo 和 authenticator 使用指令参见附录 C.12。

在公路 ETC 应用中不存在 iid 数据元。

6.3.2.5 用户提示

6.3.2.5.1 概述

提示用户交易结果。其过程如下：

——RSU：SetMMI.request；

——OBU：SetMMI.response。

6.3.2.5.2 SetMMI.request

6.3.2.5.2.1 简要说明

LLC层使用ACn命令。

APP层使用Action.request，T-APDUs= Action-Request。

本应用中，SetMMI中无需accessCredentials。

6.3.2.5.2.2 数据定义

SetMMI.request的ASN.1数据结构说明如下：

Action-Request::=SEQUENCE{

mode BOOLEAN,

did Dsrc-DID,

```
    actionType              ActionType,
    accessCredentials       OCTET STRING (SIZE(0..127,...)) OPTIONAL,
    actionParameter         Container OPTIONAL,
    iid                     Dsrc-DID OPTIONAL
    }
```

其编码规定如下：

——mode：采用确认模式，取值为1；

——did：无扩展，取值为1；

——ActionType：无扩展，取值为4；

——accessCredentials：无扩展，可选性使用；

——actionParameter：Container.Type=26（SetMMIRq），应存在。

6.3.2.5.3 SetMMI.response

6.3.2.5.3.1 简要说明

LLC层使用ACn响应。

APP层使用Action.response，T-APDUs= Action-Response。

6.3.2.5.3.2 数据定义

SetMMI.response的ASN.1数据结构说明如下：

```
Action-Response::=SEQUENCE{
    fill                    BIT STRING (SIZE(2)),
    did                     Dsrc-DID,
    responseParameter       Container OPTIONAL,
    iid                     Dsrc-DID OPTIONAL,
    ret                     ReturnStatus
    }
```

其编码规定如下：

——did，无扩展，取值为1；

——responseParameter应不存在；

——iid应不存在。

6.3.2.6 链路释放

6.3.2.6.1 概述

RSU 释放与 OBU 的通信连接。

RSU：Event-Report(Release)。

6.3.2.6.2 Event-Report(Release)

6.3.2.6.2.1 简要说明

LLC层使用UI命令，无需响应。

APP层使用Action.request，T-APDUs= event-report-request。

Event-Report(Release)用于释放OBU，让OBU进入休眠状态。

6.3.2.6.2.2 数据定义

```
Event-Report-Request::=SEQUENCE{
    mode                BOOLEAN,
    did                 DirectoryID,
    eventType           EventType,
    accessCredentials   OCTET STRING (SIZE(0..127,...)) OPTIONAL,
    eventParameter      Container OPTIONAL,
    iid                 Dsrc-DID OPTIONAL
    }
```

其编码规定如下：

——mode：采用非确认模式，取值为0；

——did：无扩展，因为Event-Report与应用无关，应取值为系统（OBU）=0；

——accessCredentials：无扩展，可选性使用；

——eventParameter：不存在；

——eventType：EventType。

7 测试方法

单片式 OBU 的测试设备、测试条件、测试方法应符合 GB/T 20851.5 及《收

费公路联网电子不停车收费技术要求》的规定。

无线电骚扰特性试验方法按照 GB/T 18655 的规定。静电放电抗扰度试验方法按照 GB/T 17626.2 的规定，接触放电电压 6kV，空气放电电压 8kV。

附录 A 应用安全

A.1 安全计算方法

A.1.1 密钥分散计算方法

由主密钥和 8 字节分散因子推导出子密钥的过程应符合下列规定：

将 16 字节主密钥 MK 对分散因子进行处理，推导出一个 16 字节长度的子密钥 DK，如图 A-1 所示。

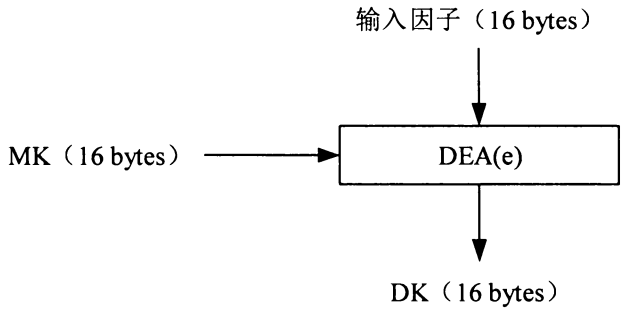


图 A-1 推导 DK

推导DK的方法是：

第一步：将分散因子按位取反，按照“分散因子”||“分散因子的反”的顺序连接在一起，组成16字节输入因子；

第二步：将 MK 作为加密密钥；

第三步：用 MK 对输入数据进行DEA加密运算。

A.1.2 数据加密的计算方法

第一步：LD（1 字节）表示明文数据的长度，在明文数据前加上 LD 产生新的数据块；

第二步：将该数据块分成 16 字节为单位的数据块，表示为 BLOCK1、BLOCK2、BLOCK3、BLOCK4 等。最后的数据块有可能是 1~16 个字节；

第三步：如果最后（或唯一）的数据块的长度是 16 字节的话，转到第四步；如果不足 16 字节，则在其后加入 0x80，如果达到 16 字节长度，则转到第四步；否则在其后加入 0x00 直到长度达到 16 字节；

第四步：按照图 A-2 所示的算法使用指定密钥对每一个数据块进行加密。

第五步：计算结束后，所有加密后的数据块依照原顺序连接在一起。

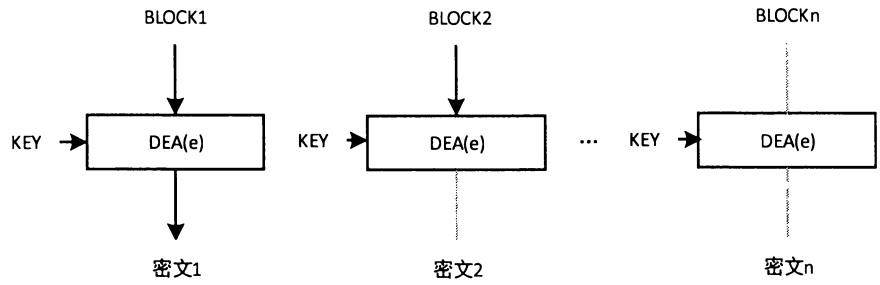


图 A-2 数据加密算法

A.1.3 过程密钥的计算方法

过程密钥的计算方法如图A-3所示，其具体步骤如下：

第一步：将输入数据In按位取反得到（~In），即（~In）= In ⊕ (0xFF||0xFF||0xFF||0xFF||0xFF||0xFF||0xFF||0xFF)，按照In||(~In)的顺序连接在一起，组成16字节输入数据；

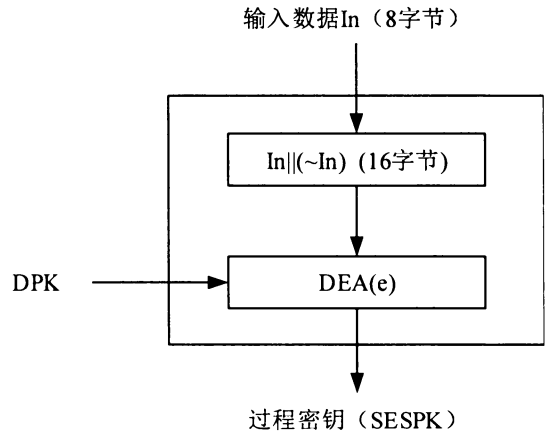


图 A-3 过程密钥的产生

第二步：将DPK作为加密密钥；

第三步：用DPK对In||(~In)进行DEA加密运算得到过程密钥。

A.1.4 安全报文的计算方法

1 命令安全报文中的 MAC 应符合下列规定：

第一步：终端通过向 OBE-SAM 发 GET CHALLENGE 命令获得一个 4字节随机数，后补 12 字节 0x00 作为初始值；

第二步：将 5字节命令头（CL A，INS，P1，P2，Lc）和命令数据域中的

明文或密文数据连接在一起形成数据块。这里的 Lc 应是数据长度加上将计算出的 MAC 的长度（4字节）后得到的实际长度；

第三步：将该数据块分成 16 字节为单位的数据块，表示为 BLOCK1、BLOCK2、 BLOCK3、BLOCK4 等。最后的数据块有可能是 1~16 字节；

第四步：如果最后的数据块的长度是 16 字节的话，则在该数据块之后再加一个完整的 16 字节数据块 0x80000000000000000000000000000000'，转到第五步；如果最后的数据块的长度不足 16 字节，则在其后加入 0x80，如果达到 16 字节长度，则转到第五步；否则接着在其后加入 0x00 直到长度达到 16 字节。

第五步：按图 A-4 所示的算法对这些数据块使用指定密钥进行加密来产生 MAC。

第六步：最终取计算结果高 4字节作为 MAC。

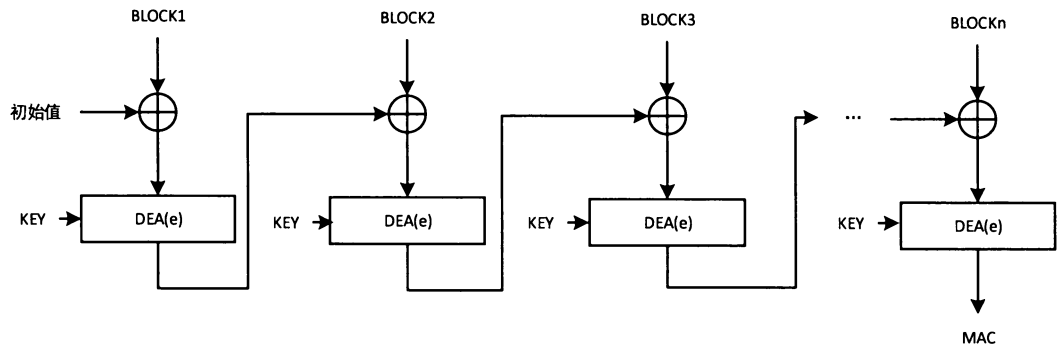


图 A-4 MAC 算法

2 鉴别码 authenticator 的计算应符合下列规定：

1）将输入数据进行 CRC 计算（多项式 $X^{16}+X^{12}+X^5+1$，起始 0xFFFF），产生两字节 CRC0 和 CRC1；

2）将送入的随机数(8bytes)最低两字节分别更换为 CRC1、CRC0，形成 8 字节临时数据；

3）使用指定交易密钥对（8 字节数据后补 8 字节 0x00 后组成的 16 字节数据）进行加密计算：Enc = SM4(LTK，CRC0||CRC1||Rand(高 6 字节)||0x0000000000000000)，authenticator=16 字节密文 Enc 前后 8 字节进行异或的结果，长度为 8 字节。

3　TAC 计算方法应符合下列规定：

1）TAC 的计算不采用过程密钥方式。

2）直接使用 TAC 密钥按照如下方式计算 TAC：

第一步：将 16 字节 0x00 设定为初始值；

第二步：将所有输入数据按指定顺序连接成一个数据块；

第三步：将该数据块分成 16 字节为单位的数据块，表示为 BLOCK1、BLOCK2、BLOCK3、BLOCK4 等。最后的数据块有可能是 1~16 个字节；

第四步：如果最后的数据块的长度是 16 字节的话，则在该数据块之后再加一个完整的 16 字节数据块 0x80000000000000000000000000000000，转到第五步；如果最后的数据块的长度不足 16 字节，则在其后加入 0x80，如果达到 16 字节长度，则转到第五步；否则在其后加入 0x00 直到长度达到 16 字节；

第五步：按照 A-4 所示的算法对这些数据块使用 TAC 密钥进行加密来产生 MAC；

第六步：最终取计算结果（高 4字节）作为 TAC。

A.2　认可的加密算法

SM4 算法应遵从《SM4 分组密码算法》GM/T 0002 的规定。

附录 B OBE-SAM 封装

B.1 OBE-SAM 封装及管脚定义

OBE-SAM 封装形式如图 B-1 所示。

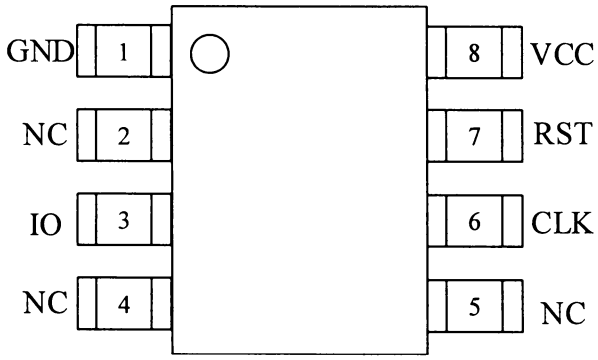


图 B-1 OBE-SAM 封装示意图

OBE-SAM 管脚定义如下表 B-1 所示。对于不同的通信协议如 SPI 协议，厂商可自行定义复用管脚。

表 B-1 OBE-SAM 管脚定义

序号	名称	类型	描述说明
1	GND	电源	地
2	NC		
3	IO	数字输入/输出	双向数据信号（内置上拉电阻）
4	NC		
5	NC		
6	CLK	数字输入	ISO/IEC 7816 时钟信号
7	RST	数字输入	复位信号，低电平有效
8	VCC	电源	电源

B.2 OBE-SAM 关键尺寸定义

OBE-SAM 关键尺寸标注如图 B-2 所示：

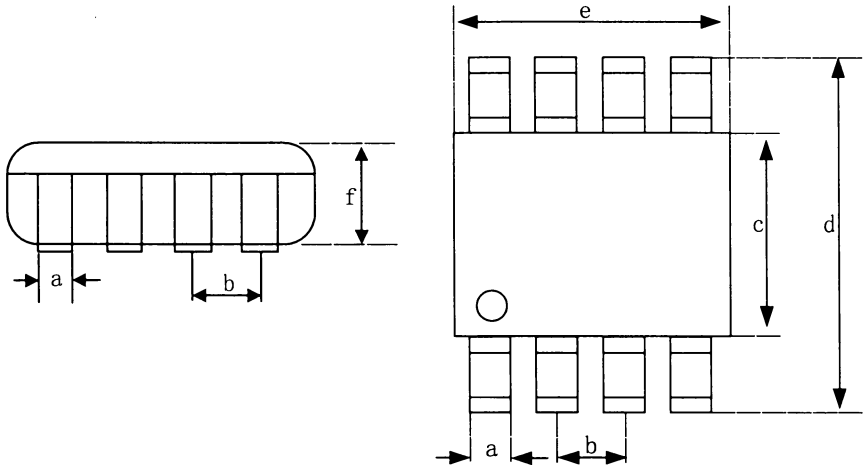


图 B-2 OBE-SAM 关键尺寸标注

OBE-SAM 关键尺寸如表 B-2 所示。

表 B-2 OBE-SAM 关键尺寸定义

标志	尺寸(毫米)			尺寸(英寸)		
	最小	标称值	最大	最小	标称值	最大
a	0.3	0.4	0.55	0.012	0.016	0.022
b	-	1.27	-	-	0.050	-
c	3.75	3.95	4.15	0.148	0.156	0.163
d	5.7	6.0	6.3	0.224	0.236	0.248
e	4.72	4.92	5.12	0.186	0.194	0.202
f	1.3	1.5	1.7	0.051	0.059	0.067

附录 C OBE-SAM 应用命令集

C.1 DECREASE COUNTER 命令应符合下列规定

DECREASE COUNTER 命令每成功执行一次，拆卸次数（即拆卸状态的低 4 位）应减 1。

DECREASE COUNTER 命令报文应符合表 C-1 的规定：

表 C-1 DECREASE COUNTER 命令报文

代码	数　值
CLA	‘00’
INS	‘59’
P1	‘00’
P2	‘00’
Lc	不存在
DATA	不存在
Le	‘01’

DECREASE COUNTER 命令报文数据域不存在。

DECREASE COUNTER 命令响应报文数据域应为剩余次数。

DECREASE COUNTER 命令响应报文状态码应符合表 C-2 的规定：

表 C-2 DECREASE COUNTER 响应报文状态码

SW1	SW2	说　明
‘90’	‘00’	命令执行成功
‘65’	‘81’	写 EEPROM 失败
‘67’	‘00’	Lc 长度错误
‘69’	‘85’	使用条件不满足，拆卸次数已经为 0
‘6A’	‘81’	功能不支持
‘6A’	‘82’	未找到文件
‘6A’	‘86’	P1、P2 参数错
‘6D’	‘00’	命令不存在
‘6E’	‘00’	CLA 错
‘93’	‘03’	应用永久锁定

C.2 EXTERNAL AUTHENTICATE 命令应符合下列规定

EXTERNAL AUTHENTICATE 命令执行成功后，应使外部接口设备对 OBE-SAM 获得某种操作授权。

接口设备提供的认证数据应按以下规则产生：

用 GET CHALLENGE 命令向 IC 卡申请一组随机数；

用指定密钥对随机数（后面填充 0x00 至 16 字节后）做加密运算产生。

认证数据为 16 字节密文前后 8 字节进行异或的结果，长度仍为 8 字节。

密钥验证失败时相应外部认证密钥的错误计数器应减 1，当计数器减为‘0’值时，密钥被锁定。

EXTERNAL AUTHENTICATE 命令报文格式应符合表 C-3 的规定：

表 C-3 EXTERNAL AUTHENTICATION 命令报文

代码	数　值
CLA	‘00’
INS	‘82’
P1	‘00’
P2	外部认证密钥标识
Lc	‘08’
Data	认证数据
Le	不存在

命令响应报文状态码应符合表 C-4 的规定：

表 C-4 EXTERNAL AUTHENTICATION 响应报文状态码

SW1	SW2	含　义
‘90’	‘00’	命令执行成功
‘63’	‘CX’	认证失败，‘X’为剩余的可尝试次数
‘67’	‘00’	Lc 不正确
‘69’	‘83’	认证方法锁定
‘69’	‘88’	OPNK 认证失败
‘6A’	‘86’	参数 P1 P2 不正确
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误

C.3　GET CHALLENGE 命令应符合下列规定

GET CHALLENGE 命令请求一个用于安全相关过程(例如安全报文)的随机数，该随机数只能用于下一条指令，无论下一条指令是否使用了该随机数，该随机数都将立即失效。

GET CHALLENGE 命令报文应符合表 C-5 的规定。

表 C-5 GET CHALLENGE 命令报文

代码	数　值
CLA	‘00’
INS	‘84’
P1	‘00’
P2	‘00’
Lc	不存在
DATA	不存在
Le	‘04’,‘08’,‘10’

GET CHALLENGE 命令响应报文数据域为随机数，长度为 4 字节或 8 字节或 16 字节。

GET CHALLENGE 命令响应报文状态码应符合表 C-6 的规定：

表 C-6 GET CHALLENGE 响应报文状态码

SW1	SW2	说　明
‘90’	‘00’	命令执行成功
‘67’	‘00’	Le 长度错误
‘6A’	‘81’	功能不支持
‘6A’	‘86’	P1、P2 参数错
‘6D’	‘00’	命令不存在
‘6E’	‘00’	CLA 错

C.4　GET RESPONSE 命令应符合下列规定

当 APDU 不能用现有协议传输时，GET RESPONSE 命令提供了一种从 OBE-SAM 向接口设备传送 APDU（或 APDU 的一部分）的传输方法。

GET RESPONSE 命令报文应符合表 C-7 的规定。

表 C-7 GET RESPONSE 命令报文

代码	数　值
CLA	‘00’
INS	‘C0’
P1	‘00’
P2	‘00’
Lc	不存在
DATA	不存在
Le	响应的最大数据长度

GET RESPONSE 命令响应报文数据域长度由 Le 的值决定。如果 Le 的值为零，在附加数据有效时，OBE-SAM 应回送状态码‘6CXX’，否则回送状态码‘6F00’。

OBE-SAM 回送的响应信息中出现的状态码应符合表 C-8 的规定。

表 C-8 GET RESPONSE 响应报文状态码

SW1	SW2	说　明
'90'	'00'	命令执行成功
'61'	'XX'	还有 'XX' 字节需要返回
'62'	'81'	回送数据有错
'67'	'00'	Lc 或 Le 长度错误
'6A'	'86'	P1、P2 参数错
'6C'	'XX'	长度错误，'XX'表示实际长度
'6D'	'00'	命令不存在
'6E'	'00'	CLA 错
'6F'	'00'	数据无效

C.5　GET SN 命令应符合下列规定

GET SN 命令用于读取 OBE-SAM 安全模块中卡商惟一的芯片序列号。

GET SN 命令执行无权限限制。

GET SN 命令报文应符合表 C-9 的规定。

表 C-9 GET SN 命令报文

代码	数　值
CLA	'80'
INS	'F6'
P1	'00'
P2	'03'
Lc	不存在
DATA	不存在
Le	'04'

GET SN 命令响应报文数据域包括 4 字节芯片序列号。

OBE-SAM 回送的响应信息中出现的状态码应符合表 C-10 的规定：

表 C-10 GET SN 响应报文状态码

SW1	SW2	说　明
'90'	'00'	命令执行成功
'6A'	'86'	P1、P2 参数错
'6C'	'XX'	Le 长度错误，'XX' 表示实际长度
'6D'	'00'	命令不存在
'6E'	'00'	CLA 错

C.6 READ BINARY 命令

READ BINARY 命令用于读出二进制文件的内容（或部分内容）。

READ BINARY 命令报文应符合表 C-11 的规定。

表 C-11 READ BINARY 命令报文

代码	数 值								
CLA	'00'或'04'								
INS	'B0'								
P1	b8	b7	b6	b5	b4	b3	b2	b1	说 明
	0	X	X	X	X	X	X	X	当前文件高位地址
	1	0	0	X	X	X	X	X	通过 SFI 方式访问
P2	若 P1 的 b8=0，P2 为文件的低位地址 若 P1 的 b8=1，P2 为文件地址								
Lc	1）不存在——明文方式 2）'04'——校验方式								
DATA	1）不存在 2）MAC								
Le	期望返回的数据长度								

READ BINARY 命令使用 SFI 读取文件后，该文件成为当前文件。

READ BINARY 命令报文数据域一般情况下不存在。当使用安全报文时，命令报文数据域中应包含 MAC。MAC 的计算方法和长度应符合附录 A 的规定。

READ BINARY 命令响应报文数据域，当 Le 的值为零时，当从指定的偏移量至文件结束，长度小于 256 字节、等于 256 字节、大于 256 字节时，返回数据长度应符合表 C-12 的规定

表 C-12 Le=0 时的命令响应信息

实际长度	小于 256 字节	等于 256 字节	大于 256 字节
返回数据	6CXX，其中 XX 为实际长度	返回 256 字节	返回 256 字节

OBE-SAM 回送的响应信息中的状态码应符合表 C-13 的规定。

表 C-13 READ BINARY 响应报文状态码

SW1	SW2	说 明
'90'	'00'	命令执行成功
'61'	'XX'	还有 'XX' 字节要返回
'62'	'81'	部分回送的数据有错
'62'	'82'	文件长度<Le
'65'	'81'	写 EEPROM 失败
'67'	'00'	Lc 长度错误

‘69’	‘81’	当前文件不是二进制文件
‘69’	‘82’	不满足安全状态
‘69’	‘83’	认证密钥锁定
‘69’	‘84’	引用数据无效（未申请随机数）
‘69’	‘85’	使用条件不满足
‘69’	‘86’	没有选择当前文件
‘69’	‘88’	安全信息（MAC 和加密）数据错误
‘6A’	‘81’	功能不支持
‘6A’	‘82’	未找到文件
‘6A’	‘86’	P1、P2 参数错
‘6A’	‘88’	未找到密钥数据
‘6B’	‘00’	起始地址超出范围
‘6C’	‘XX’	Le 长度错误。‘XX’表示实际长度
‘6D’	‘00’	命令不存在
‘6E’	‘00’	CLA 错
‘93’	‘03’	应用永久锁定

C.7 READ RECORD 命令应符合下列规定

READ RECORD 命令读记录文件中的内容。

READ RECORD 命令报文应符合表 C-14 的规定。

表 C-14 READ RECORD 命令报文

<table>
<tr><td>代码</td><td colspan="9">数 值</td></tr>
<tr><td>CLA</td><td colspan="9">‘00’或‘04’</td></tr>
<tr><td>INS</td><td colspan="9">‘B2’</td></tr>
<tr><td>P1</td><td colspan="9">记录号</td></tr>
<tr><td rowspan="5">P2</td><td>b8</td><td>b7</td><td>b6</td><td>b5</td><td>b4</td><td>b3</td><td>b2</td><td>b1</td><td>说 明</td></tr>
<tr><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>-</td><td>-</td><td>-</td><td>当前文件</td></tr>
<tr><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>-</td><td>-</td><td>-</td><td>通过 SFI 方式访问</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>-</td><td>-</td><td>1</td><td>0</td><td>0</td><td>P1 指定的记录号</td></tr>
<tr><td colspan="8">其他值</td><td>保留</td></tr>
<tr><td>Lc</td><td colspan="9">1) 不存在——明文方式
2) ‘04’ —— 命令报文校验方式</td></tr>
<tr><td>DATA</td><td colspan="9">1）不存在——明文方式
2）MAC——校验方式</td></tr>
<tr><td>Le</td><td colspan="9">期望返回的记录数据</td></tr>
</table>

READ RECORD 命令使用 SFI 读取文件后，该文件成为当前文件。

一般情况下命令报文数据域不存在。当使用安全报文时，命令报文数据域中应包含 MAC。MAC 的计算方法和长度由应用决定。

所有执行成功的 READ RECORD 命令的响应报文数据域由读取的记录组成。

OBE-SAM 回送的响应信息中的状态码应符合表 C-15 的规定。

表 C-15 READ RECORD 响应报文状态码

SW1	SW2	说　明
'90'	'00'	命令执行成功
'61'	'XX'	还有 'XX' 字节需要返回
'62'	'81'	回送的数据有错
'64'	'00'	标志状态位没变
'65'	'81'	写 EEPROM 失败
'67'	'00'	Lc 长度错误
'69'	'81'	当前文件不是记录文件
'69'	'82'	不满足安全状态
'69'	'83'	认证密钥锁定
'69'	'84'	引用数据无效(未申请随机数)
'69'	'85'	使用条件不满足
'69'	'86'	没有选择当前文件
'69'	'88'	安全信息（MAC 和加密）数据错误
'6A'	'81'	功能不支持
'6A'	'82'	未找到文件
'6A'	'83'	未找到记录
'6A'	'85'	Lc 与 TLV 结构不匹配
'6A'	'86'	P1、P2 参数错
'6A'	'88'	未找到密钥数据
'6C'	'XX'	Le 错误，'XX'表示实际长度
'6D'	'00'	命令不存在
'6E'	'00'	CLA 错
'93'	'03'	应用永久锁定

C.8　SELECT FILE 命令应符合下列规定

SELECT FILE 命令通过文件标识或应用名选择 OBE-SAM 中的 MF、DDF、ADF 或 EF 文件。

成功执行该命令设定 MF、DDF 或 ADF 的路径。

应用到 EF 的后续命令将采用 SFI 方式联系到所选定的 MF、DDF 或 ADF。

从 OBE-SAM 返回的应答报文包含回送 FCI。

FCI 数据从数据分组中获得。

SELECT FILE 命令报文应符合表 C-16 的规定。

表 C-16 SELECT FILE 命令报文

代码	数　值
CLA	'00'
INS	'A4'
P1	'00'通过 FID 选择 DF、EF，当 Lc='00'时，选 MF '04'通过 DF 名选择应用
P2	'00' '02'选择下一个文件（P1=04h 时）
Lc	P1='00'时，Lc='00'或'02' P1='04'时，Lc='05'~'10'
DATA	文件标识符（FID—2 字节） 应用名（App-Name，P1='04'）
Le	FCI 文件的信息长度（选择 DF 时）

命令报文数据域应包括所选择的 DDF 名、DF 名或 FID，以及 EF 的 FID。

响应报文数据域中的数据应包括所选择的 MF、DDF、ADF 的 FCI。

成功选择 MF 后回送的 FCI 应符合表 C-17 的规定。

表 C-17 成功选择 MF 响应报文 FCI

标识	数　值			存在性
'6F'	FCI 模板			M
	'84'	DF		M
	'A5'	FCI 数据专用模板		M
		'88'	目录基本文件的 SFI	O
		'9F0C'	FCI 文件内容	O

成功选择 DDF 后回送的 FCI 应符合表 C-18 的规定。

表 C-18 成功选择 DDF 响应报文 FCI

标签	数　值			存在性
'6F'	FCI 模板			M
	'84'	DF 名		M
	'A5'	FCI 数据专用模板		M
		'88'	目录基本文件的 SFI	O
		'9F0C'	FCI 文件内容	O

成功选择 ADF 后回送的 FCI 应符合表 C-19 的规定。

表 C-19 成功选择 ADF 响应报文 FCI

标签	数　值	存在性

'6F'	FCI 模板		M
	'84'	DF 名	M
	'A5'	FCI 数据专用模板	M
	'9F0C'	FCI 文件内容	O

OBE-SAM 回送的响应信息中的状态码应符合表 C-20 的规定。

表 C-20 SELECT FILE 响应报文状态码

SW1	SW2	说　明
'90'	'00'	命令执行成功
'62'	'83'	选择文件无效
'62'	'84'	FCI 格式与 P2 指定的不符
'64'	'00'	标志状态位没变
'67'	'00'	Lc 长度错误
'6A'	'81'	功能不支持
'6A'	'82'	未找到文件
'6A'	'86'	P1、P2 参数错
'6A'	'87'	Lc 与 P1-P2 不匹配
'6D'	'00'	命令不存在
'6E'	'00'	CLA 错
'93'	'03'	应用永久锁定

C.9 UPDATE BINARY 命令

UPDATE BINARY 命令用于更新二进制文件中的数据。

UPDATE BINARY 命令报文应符合表 C-21 的规定。

表 C-21 UPDATE BINARY 命令报文

代码	数　值								
CLA	'00'或'04'								
INS	'D6'								
P1	b8	b7	b6	b5	b4	b3	b2	b1	说　明
	0	X	X	X	X	X	X	X	当前文件高位地址
	1	0	0	X	X	X	X	X	通过 SFI 方式访问
P2	若 P1 的 b8=0，P2 为文件的低位地址 若 P1 的 b8=1，P2 为文件地址								
Lc	DATA 域数据长度								
DATA	明文方式：　明文数据 加密方式：　密文数据 校验方式：　明文数据‖校验码 校验加密方式：密文数据‖校验码								
Le	不存在								

UPDATE BINARY 命令使用 SFI 更新文件后，该文件成为当前文件。

命令报文数据域包括更新原有数据的数据域。

OBE-SAM 回送的响应信息中的状态码应符合表 C-22 的规定。

表 C-22 UPDATE BINARY 响应报文状态码

SW1	SW2	说　明
'90'	'00'	命令执行成功
'65'	'81'	写 EEPROM 失败
'67'	'00'	Lc 长度错误
'69'	'81'	当前文件不是二进制文件
'69'	'82'	不满足安全状态
'69'	'83'	认证密钥锁定
'69'	'84'	引用数据无效（未申请随机数）
'69'	'85'	使用条件不满足
'69'	'86'	未选择文件
'69'	'88'	安全信息（MAC 和加密）数据错误
'6A'	'81'	功能不支持
'6A'	'82'	未找到文件
'6A'	'86'	P1、P2 参数错
'6A'	'88'	未找到密钥数据
'6B'	'00'	起始地址超出范围
'6D'	'00'	命令不存在
'6E'	'00'	CLA 错
'93'	'03'	应用永久锁定

C.10　UPDATE RECORD 命令应符合下列规定

UPDATE RECORD 命令用于更新记录文件中的数据。

在使用当前记录地址时，该命令将在修改记录成功后重新设定记录指针。

UPDATE RECORD 命令报文应符合表 C-23 的规定。

表 C-23 UPDATE RECORD 命令报文

代码	数　值								
CLA	'00'或'04'								
INS	'DC'								
P1	P1= '00' 表示当前记录 P1≠ '00' 表示指定的记录号或记录标识								
P2	b8	b7	b6	b5	b4	b3	b2	b1	说　明
	0	0	0	0	0	-	-	-	当前文件
	X	X	X	X	X	-	-	-	通过 SFI 方式访问

	-	-	-	-	-	1	0	0	P1 指定的记录号
	-	-	-	-	-	0	0	0	第一条记录
	-	-	-	-	-	0	0	1	最后一条记录
	-	-	-	-	-	0	1	0	下一条记录
	-	-	-	-	-	0	1	1	前一条记录
	任何其他值								保留
Lc	DATA 域数据长度								
DATA	明文方式：　明文记录数据 加密方式：　密文记录数据 校验方式：　明文记录数据‖校验码 校验加密方式：密文记录数据‖校验码								
Le	不存在								

UPDATE RECORD 命令使用 SFI 更新文件后，该文件成为当前文件。

命令报文数据域由更新原有记录的新记录组成。

OBE-SAM 回送的响应信息中的状态码应符合表 C-24 的规定。

表 C-24 UPDATE RECORD 响应报文状态码

SW1	SW2	说　明
'90'	'00'	命令执行成功
'65'	'81'	写 EEPROM 失败
'67'	'00'	Lc 长度错误
'69'	'81'	当前文件不是记录文件
'69'	'82'	不满足安全状态
'69'	'83'	认证密钥锁定
'69'	'84'	引用数据无效（未申请随机数）
'69'	'85'	使用条件不满足
'69'	'86'	未选择文件
'69'	'88'	安全信息（MAC 和加密）数据错误
'6A'	'81'	功能不支持
'6A'	'82'	未找到文件
'6A'	'83'	未找到记录
'6A'	'84'	存储空间不够
'6A'	'85'	Lc 与 TLV 结构不匹配
'6A'	'86'	P1、P2 参数错
'6A'	'88'	未找到密钥数据
'6D'	'00'	命令不存在
'6E'	'00'	CLA 错
'93'	'03'	应用永久锁定

C.11 UPDATE KEY 命令应符合下列规定

UPDATE KEY 命令用于更新一个已经存在的密钥。

本命令可支持 16 字节的密钥，密钥写入应采用密文+MAC 的方式，在主控密钥的控制下进行。

在密钥装载前应用 GET CHANLLEGE 命令从 OBE-SAM 取一个 4 字节的随机数。

UPDATE KEY 命令报文应符合表 C-25 的规定。

表 C-25 UPDATE KEY 命令报文

代 码	数 值
CLA	'84'
INS	'D4'
P1	'01'
P2	'00'--更新主控密钥 'FF'--更新其他密钥
Lc	'24'
DATA	密文密钥信息‖MAC
Le	不存在

命令报文数据域包括要装载的密钥密文信息和 MAC。密钥密文信息是用主控密钥对以下数据加密（按所列顺序）产生的：

——密钥用途

——密钥标识

——密钥值

MAC 是用主控密钥对以下数据进行 MAC 计算（按所列顺序）产生的：

——CLA

——INS

——P1

——P2

——Lc

——密钥密文信息

响应信息中的状态码应符合表 C-26 的规定。

表 C-26 UPDATE KEY 响应报文状态码

SW1	SW2	含　义
‘90’	‘00’	命令执行成功
‘65’	‘81’	写 EEPROM 失败
‘67’	‘00’	Lc 长度错误
‘69’	‘82’	不满足安全状态
‘69’	‘83’	认证密钥锁定
‘69’	‘84’	引用数据无效（未申请随机数）
‘69’	‘85’	使用条件不满足
‘69’	‘88’	安全信息（MAC 和密文）数据错误
‘6A’	‘80’	数据域参数错误
‘6A’	‘81’	功能不支持
‘6A’	‘82’	未找到文件
‘6A’	‘83’	未找到密钥数据
‘6A’	‘84’	文件空间已满
‘6A’	‘86’	P1、P2 参数错
‘6A’	‘88’	未找到密钥数据
‘6D’	‘00’	命令不存在
‘6E’	‘00’	CLA 错
‘93’	‘03’	应用永久锁定

C.12　LANE TRANSACTION 命令应符合下列规定

该命令在车道交易中完成 TAC 码计算，生成鉴别码 authenticator，并可选地写入当次过站信息。执行该命令时，需满足相应的操作权限：当交易类型为 ‘8X’ 时，应满足 $OPNK11_{\_DF01}$ 或 $OPNK12_{\_DF01}$ 认证成功后的状态；当交易类型为‘9X’ 时，应满足 $OPNK21_{\_DF01}$ 或 $OPNK22_{\_DF01}$ 认证成功后的状态。

LANE TRANSACTION 命令报文格式应符合表 C-27 的规定。

表 C-27 LANE TRANSACTION 命令报文格式

代码	数　值
CLA	‘80’
INS	‘FC’
P1	‘XX’，交易类型
P2	‘XX’，　LTK 密钥标识
Lc	‘XX’
Data	P1= ‘80’，随机数（8 字节）+交易金额（4 字节）+终端机编号（6 字节）+终端交易序号（4 字节）+交易日期时间（7 字节）+ETC 门架编号（3 字节）+车型（1 字节） P1= ‘81’，随机数（8 字节）+交易金额（4 字节）+终端机编号（6 字节）+终端交易序号（4 字节）+交易日期时间（7 字节）+ 收费站编号（3 字节）+车型（1 字节）+收费公路 ETC 应用入 / 出口信息文件偏移量（2 字节，从 0 开始）+收费公路 ETC 应用入 / 出口信息文件长度（1 字节，值为 N）+收费公路 ETC 应用入 / 出口信息文件内

	容（N 字节） P1= ‘90’，随机数（8 字节）+交易金额（4 字节）+终端机编号（6 字节）+终端交易序号（4 字节）+交易日期时间（7 字节）+ 收费站编号（3 字节）+车型（1 字节）+其他封闭式应用入 / 出口信息文件偏移量（2 字节，从 0 开始）+其他封闭式应用入 / 出口信息文件长度（1 字节，值为 N）+其他封闭式应用入 / 出口信息文件内容（N 字节）
Le	Le = ‘0C’
响应数据	Authenticator+TAC

其中交易类型定义见表 C-28。“过站信息”是指写入“封闭式应用入 / 出口信息文件”的数据。

表 C-28 交易类型定义

交易类型数值	说明
0x80	收费公路自由流交易
0x81	收费公路封闭式交易
0x90	其他封闭式应用交易

authenticator 和 TAC 的计算方法见附录 A.1.4.

authenticator 和 TAC 的计算数据域参见 GetTollData 和 SetTollData 原语。

响应信息中的状态码应符合表 C-29 的规定。

表 C-29 响应信息中的状态码

SW1	SW2	含义
‘90’	‘00’	命令执行成功
‘65’	‘81’	内存失败
‘67’	‘00’	长度错误
‘69’	‘82’	不满足安全状态
‘6A’	‘86’	参数 P1，P2 不正确
‘6D’	‘00’	命令不存在
‘6E’	‘00’	CLA 错

C.13 GENERATE AUTHENTICATOR 命令应符合下列规定

本命令用于生成符合 DSRC 协议安全认证要求信息鉴别码 authenticator，执行该命令时，需满足任一条 OPNK 认证成功后的状态。命令报文格式应符合表 C-30 的规定。

表 C-30 GENERATE AUTHENTICATOR 命令报文格式

代码	数　值
CLA	‘80’

INS	‘FA’
P1	‘00’
P2	‘XX’，LTK 密钥标识
Lc	‘XX’
Data	随机数（8 字节）+ FILE（待处理的数据内容）
Le	Le=‘08’
响应数据	Authenticator

OBE-SAM 使用 P2 指定密钥对 FILE 数据域进行鉴别码 authenticator 计算，其计算方法见附录 A.1.4。

响应信息中的状态码应符合表 C-31 的规定。

表 C-31 响应信息中的状态码

SW1	SW2	含义
‘90’	‘00’	命令执行成功
‘65’	‘81’	内存失败
‘67’	‘00’	长度错误
‘69’	‘82’	不满足安全状态
‘6A’	‘86’	参数 P1，P2 不正确
‘6D’	‘00’	命令不存在
‘6E’	‘00’	CLA 错

分送：各省、自治区、直辖市、新疆生产建设兵团交通运输厅(局、委)。

交通运输部办公厅　　2019年5月27日印发